Software Engineering Institute

Study of Integration Considerations for Wireless Emergency Alerts

The WEA Project Team

February 2014

SPECIAL REPORT
CMU/SEI-2013-SR-016

CERT® Division, Software Solutions Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

DM-0000453

Table of Contents

List of Figures

List of Tables

Acknowledgments

We thank the following organizations for their help and feedback during data collection:

Emergency Management Organizations

- Adams County 911, Colorado
- Alachua County Fire Rescue, Florida
- Altus Emergency Management Agency, Oklahoma
- Arvada Police Department, Colorado PUC 911 Task Force
- California Emergency Management Agency (Cal EMA)
- Cecil County Emergency Management Services, Maryland
- Colorado Office of Emergency Management
- Commonwealth Interoperability Coordinator's Office, Virginia
- Dane County Emergency Management, Wisconsin
- Emergency Management and Homeland Security, Lakewood, Colorado
- Fairfax County Office of Emergency Management, Virginia
- Harris County Office of Homeland Security and Emergency Management, Texas
- Hawaii State Civil Defense
- Jefferson County Emergency Communication Authority (JCECA), Colorado
- Johnson County Emergency Management Agency, Kansas
- Larimer Emergency Telephone Authority (LETA 911), Colorado
- Lexington-Fayette Urban County Government, Kentucky
- Maine Emergency Management Agency
- Metropolitan Washington Council of Governments, Washington, D.C.
- National Center for Missing & Exploited Children, Virginia
- National Oceanic and Atmospheric Administration/National Weather Service, Sterling, Virginia
- National Oceanic and Atmospheric Administration/National Weather Service, Colorado
- New York State Division of Homeland Security and Emergency Services
- Office of Emergency Management and Homeland Security, Pittsburgh, Pennsylvania
- Office of Environmental Health & Safety, Carnegie Mellon University, Pittsburgh, Pennsylvania
- Virginia Polytechnic Institute and State University, Blacksburg, Virginia
- Washington Military Department, Emergency Management Division, Washington
- Westminster Fire Department, Westminster, Colorado

Vendors

- Alcatel-Lucent
- AtHoc/Alerting Solutions
- Buffalo Computer Graphics
- Cassidian Communications
- CMAS Holdings, LLC
- ComLabs
- Digital Alert Systems
- Emergency Communications Network
- ESi Acquisition, Inc.
- Everbridge
- Eye Street Solutions
- NC4
- TeleCommunication Systems (TCS)
- Wide Area Rapid Notification (W.A.R.N.)

Other Organizations and Sources

- Art Botterell, Carnegie Mellon University, Silicon Valley, California
- Department of Homeland Security Science and Technology Directorate, Washington, D.C.
- EAS Committee, Wisconsin
- National Consortium for the Study of Terrorism and Responses to Terrorism (START), Maryland
- Rice Consulting Services, Oklahoma
- Wisconsin AMBER Alert Committee

We also thank several emergency management organizations, vendors, and emergency alert experts that wish to remain anonymous.

Executive Summary

The Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS), is a collaborative partnership that includes the cellular industry, the Federal Communications Commission, the Federal Emergency Management Agency, and the Department of Homeland Security Science and Technology Directorate (DHS S&T).[1] This report, *Study of Integration Strategy Considerations for Wireless Emergency Alerts*, supports the WEA Research, Development, Testing, and Evaluation program by identifying and analyzing key WEA adoption issues. Because each organization's situation is different, emergency management agencies (EMAs) should adapt the information in this report to build their own WEA integration strategies to enable the successful deployment, operations, and sustainment of the WEA capability.

This report presents the results of a study performed in partnership with the EMA community. The results are generalized from interactions with a wide array of WEA stakeholders that included small EMAs, university emergency managers, city and county EMAs, state-level EMAs, territories, national alerting organizations, vendors of systems for issuing WEA messages, Common Alerting Protocol (CAP) standard experts, and people building open-source alerting systems. The goal of the study was to capture key challenges for WEA message originators and make recommendations to help the community avoid common pitfalls as it plans and implements the adoption and integration of WEA services with existing mobile alert and warning systems and tools.

The first four sections of this report provide context and take a high-level view of WEA adoption. Section 1 describes the scope of this study and summarizes the research method, introducing the grounded theory approach [Corbin 2008] used for this study. Section 2 discusses the current strengths and challenges of WEA as they relate to adopting a WEA messaging solution. EMAs have a strong desire to leverage mobile devices for public alerting, and this section provides a list of potential barriers to doing so as well as some ways to mitigate these barriers. Section 3 situates WEA as one of many alerting systems to be integrated into the alert originator's (AO's) toolbox, which includes emergency management and incident-warning solutions, and discusses how this may affect adoption. Section 4 presents a list of overall considerations for integrating a WEA messaging solution into an existing emergency management system. As alerting technology evolves, and as EMA jurisdictions grow and change, the scale and need for coordination increases.

The subsequent seven sections of the report each focus on a key topic for WEA adoption and on recommendations for AOs.

- Section 5 discusses technical requirements considerations for EMAs integrating WEA messaging solutions into their existing mobile alert and warning systems and tools. Technical requirements are statements of what a system must do and how it must behave, and EMAs should communicate their needs to vendors or developers in clear requirement statements. Examples illustrate how to specify better requirements.

[1] The FCC formerly referred to WEA as the Personal Localized Alerting Network (PLAN). DHS and the FCC later adopted the name preferred by commercial mobile service providers—WEA.

- Section 6 covers trends and considerations related to cloud-based solutions. The EMA community is rapidly moving toward cloud-based vendor products that integrate with the Integrated Public Alert and Warning System Open Platform for Emergency Network (IPAWS-OPEN). This section points out common pitfalls of cloud-based WEA solutions and provides recommendations for avoiding them.
- Section 7 summarizes WEA security considerations. It recommends a cybersecurity risk-management strategy focused on preventing, detecting, responding to, and recovering from cyber attacks and offers a resource for further reading.
- Section 8 discusses WEA product selection. Because feature-selection decisions are also design decisions, prioritizing one desired quality in a product may negatively affect another desired quality. This section offers considerations for balancing an organization's priorities concerning WEA solutions.
- Section 9 identifies testing considerations for WEA. It provides an overview of the testing options available through FEMA and suggests several levels of system testing that EMAs should perform.
- Section 10 addresses operational considerations. EMAs need to identify the impact of WEA adoption on their operations before an emergency event occurs. This section discusses challenges and recommendations for making WEA part of operations, messaging practices, and large-scale exercises. Another aspect of operational considerations involves coordinating WEA messages among local, county, and state organizations and among media outlets to warn the public. Recommendations present guidance on communication and synchronization.
- Section 11 reviews several alternatives to buying a WEA solution. This section addresses AOs who have decided to construct their own alerting solution, offering key considerations for different types of build approaches and experiences from organizations that have developed their own solutions.

The report concludes with a brief summary and discussion of some future considerations, followed by several appendices that provide supplemental information on the research approach and method of data collection; a step-by-step framework for WEA adoption; further information on testing considerations, illustrated with an example; examples of WEA requirements that we collected; and a list of useful resources.

Engagements with the emergency-management community, vendors, and consultants provided concrete examples of the challenges and barriers to WEA adoption for all the key topics of this report. This informed and enabled the construction of recommendations for resolving these challenges to help integrate WEA into EMAs' alerting capabilities. The resulting considerations for adoption should be a helpful resource for AOs while they integrate a WEA tool or service into their operations. Because each organization's situation is different, EMAs should adapt the information in this report and build their own WEA integration strategies to enable AOs to successfully deploy, operate, and sustain the WEA capability.

Abstract

This report supports the Wireless Emergency Alerts (WEA) program, formerly known as the Commercial Mobile Alert Service Research, Development, Testing, and Evaluation program, by identifying and analyzing key WEA adoption issues. The study captures key challenges for WEA message originators and offers recommendations to help the community avoid common pitfalls as it plans and implements the WEA service. The report summarizes the current strengths and challenges of WEA, how WEA fits into the alert originator's toolbox, and overall considerations for integrating a new WEA tool or service into an emergency management system as that system becomes ever more complex. The report also covers key topics for adopting a WEA tool or service, including requirements specification, cloud trends, cybersecurity, product selection, testing, coordinating among tools and alerting organizations, operational considerations, and alternatives to buying a WEA solution. For each of these topics, recommendations offer guidance that emergency management agencies can use to navigate the process of adopting and integrating WEA into their alerting capabilities.

1 Introduction

1.1 Background

The attacks of September 11, 2001, underscored problems in the U.S. telecommunications infrastructure under emergency conditions. While various emergency agencies struggled with their own problems of communication and coordination, the public quickly discovered that the cell phone networks were overwhelmed. Cell phone traffic was double that of normal loading, causing problems not only in New York City and Washington, D.C., but also along other parts of the East Coast. More recently, the Lower North Fork fire of March 2012 in Colorado caused three fatalities, and some alert originators we interviewed hypothesized that failures in the landline-based telephone alerting systems may have contributed to the severity of the outcome. A local television station reported that incorrect records in a geographic database were responsible for many of the failures. And the *Denver Post* report on the June 2012 Waldo Canyon fire near Colorado Springs revealed similar problems in the emergency alerting systems. Complicating the traditional alerting process, more than 35%[2] of U.S. homes do not have land-based phone lines.

Given the mobile nature of today's society, the emergency alert and response community and all levels of government knew that the United States needed a better solution to warn people of imminent threats by using geographic data. In 2006, the federal government passed the Warning, Alert, and Response Network (WARN) Act to establish a unified national hazard-alert system. One part of the response was the authorization of the Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS) Research, Development, Testing, and Evaluation (RDT&E) program.

The WEA RDT&E program is a collaborative partnership that includes the cellular industry, the Federal Communications Commission (FCC), the Federal Emergency Management Agency (FEMA), and the Department of Homeland Security Science and Technology Directorate (DHS S&T). The impact of WEA extends far beyond these agencies. WEA coexists with other alerting programs including those of the National Weather Service (NWS), the Emergency Alert System (EAS), and a growing number of private services on college and business campuses. There is a sociotechnical ecosystem growing up around WEA that encompasses the technologies and people related to alerting standards; alerting infrastructures; and local, state, territorial, and federal emergency management agencies. Figure 1 represents the elements in the ecosystem and their interactions. Alert originators (AOs) encounter these interactions in the form of rules, regulations, and contracts for services and equipment. Later in this document, we describe some of those interactions and how they affect what emergency management agencies can, should, and must do with respect to conducting exercises and issuing alerts. More information about the ecosystem is available in the report *CMAS Alerting Pipeline Taxonomy* [SEI 2012].

[2] As of December 2012. This figure is tracked each year by the Centers for Disease Control and Prevention. This is a 77% increase over late 2008 [Santana 2013].

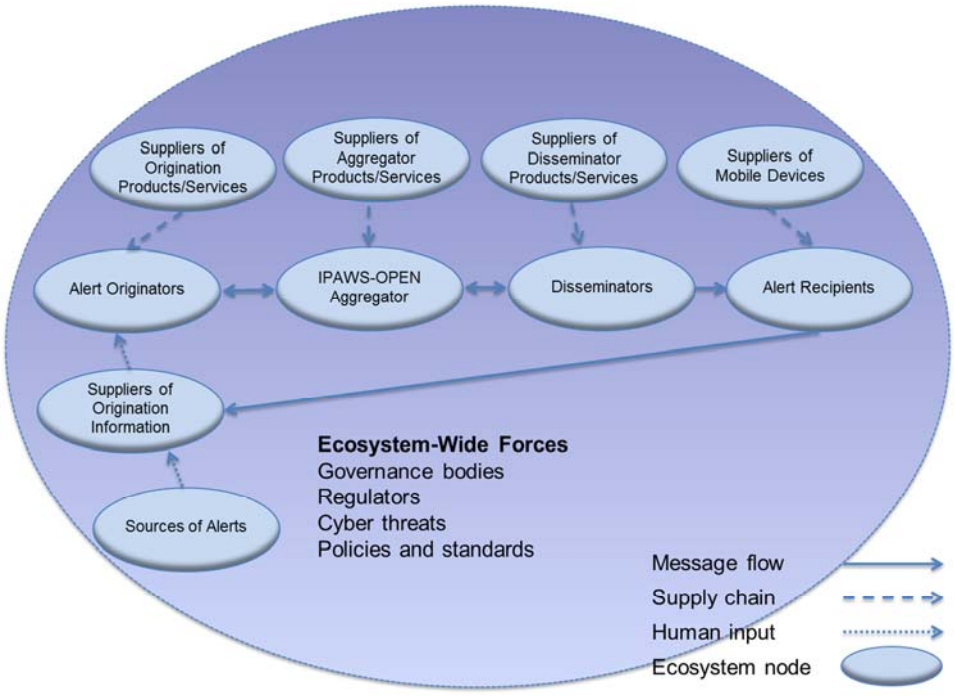


Figure 1: Ecosystem in Which WEA Operates

WEA uses existing commercial telecommunication infrastructures to broadcast emergency alerts. It supports three types of emergency alerts: Presidential, Imminent Threat, and America's Missing: Broadcast Emergency Response (AMBER) Alerts.

WEA message originators use an open, nonproprietary digital message format called the CAP. CAP is an international standard developed by the Organization for the Advancement of Structured Information Standards (OASIS) [OASIS 2007, 2010]. FEMA has adopted CAP, Version 1.2, for use in the Integrated Public Alert and Warning System Open Platform for Emergency Network (IPAWS-OPEN) [OASIS 2009]. This standardized message format fosters alerting system compatibility over multiple communication methods. CAP also has the capacity to support information such as images, audio, video, and geospatial data.

This report presents the results of a study performed in partnership with the WEA emergency management agency (EMA) community. The results we present are generalized from interactions with a wide array of WEA stakeholders that included university emergency managers, city and county EMAs, state-level EMAs, territories, national alerting organizations, vendors of products for issuing WEA messages, CAP standard experts, and people building open-source alerting solutions. The goal of the study was to capture key challenges for WEA message originators and make recommendations to help EMAs improve results and avoid common pitfalls as they adopt the WEA service and integrate it into EMA operations. EMAs authorized (or seeking authorization) to send alerts can adapt the information in this report to build their own WEA integration strategy.

1.2 Scope

The scope of this study was the alert-origination side of the WEA messaging process. The scope did not include IPAWS-OPEN message processing or carrier dissemination. This report emphasizes technical considerations. However, it also addresses some key non-technical factors because

adopting and developing a complete integration strategy for WEA must address all factors that influence the technical implementation of alerting.

1.3 Approach

We applied a qualitative research approach based on *grounded theory*, which aims to let the results emerge from the data rather than presupposing a hypothesis or assertion [Glaser 2001]. Appendix A provides a detailed description of the research design and grounded-theory approach and includes a table that briefly profiles each organization that participated in the interviews. Grounded theory has been increasingly leveraged in the technical research community to bring rigor to qualitative data collection and analysis techniques [Adolf 2011]. Other techniques applied in this study include foundational work of the Carnegie Mellon® Software Engineering Institute (SEI) such as the Architecture Tradeoff Analysis Method® and Independent Technical Assessment processes, which have been conducted effectively on hundreds of large-scale government and industry projects all over the world.

The grounded-theory approach ensured that we focused on the things that pose real challenges to EMAs. The research approach began with a guiding question for this study: "What are the AOs' barriers to WEA adoption and operational use?" As noted earlier, because each organization is different, EMAs should adapt these adoption considerations to build suitable adoption strategies. We gathered data and made a set of general observations that we used to develop a structured question set for more exploratory research into key observation areas. We then combined software and system experience, study data, and well-accepted reference materials from the software and system fields to develop the recommendations. We built validation into the research approach through the constant-comparison process described in Appendix A [Corbin 2008]. In this process, we continuously compared data from interviews and considered an observation strong enough to investigate if multiple stakeholders made similar statements in independent data-gathering sessions.

1.4 Organization of the Report and Summary of Observations

This study focused on capturing challenges or barriers to adoption from the EMA perspective, particularly those related to the alerting software and systems that EMAs purchase or build to interface with IPAWS-OPEN. While reading the entire report will provide the most complete understanding of the issues, each section is largely self-contained so that the reader can investigate topics separately. This report is organized as follows:

The first four sections provide context and take a high-level view of WEA adoption. The introductory section describes the scope of the study and summarizes the research method, introducing the grounded-theory analysis approach. Section 2 discusses the current strengths and challenges of WEA as they relate to adopting a WEA tool or service and provides a list of potential barriers to adoption as well as some ways to mitigate these barriers. Section 3 situates WEA as one of many alerting systems to be integrated into the AO's toolbox, which includes emergency-management and incident-warning tools, and discusses how this may affect adoption. Section 4 covers a list of overall considerations for integrating a new WEA tool or service into an emergency-management system as that system and the scale of coordination become ever more complex.

The next seven sections each focus on a key topic for WEA adoption and offer recommendations for AOs:

- Section 5: Requirements Considerations
- Section 6: Cloud Trends for WEA Adoption
- Section 7: Cybersecurity
- Section 8: WEA Product Selection
- Section 9: Testing Considerations
- Section 10: Operational Considerations
- Section 11: Alternatives to Buying a WEA Solution

Table 1 summarizes all the observations and related recommendations.

Table 1: Summary of Observations and Recommendations

Section	WEA Topic	Observations	Recommendations
2	Adoption	• WEA has several recognized strengths that make adoption attractive to EMAs. • The EMA community has a number of common concerns about WEA, and addressing them would speed adoption.	• No recommendations. This section describes the current state of WEA.
3	Integration	• EMAs consider WEA as an augmentation to their suite of alerting tools, not as a stand-alone system.	• Consider WEA adoption from an integrated perspective.

4	Integration	• The need to integrate a variety of technologies and methods to reach the public (e.g., alerting tools, website, call centers) has increased the need for more rigor in integration design and analysis.
		• As both the scale of emergency management systems and EMAs' responsiblity increase, integration complexity increases.
			• Focus on "bigger picture" system analysis throughout the integration strategy life cycle including
			  • planning
			  • requirements identification
			  • system design and implementation
			  • test and evaluation
			  • system sustainment

5	Requirements	• EMAs struggle with communicating their requirements to vendors.
		• While "universal" functional requirements for WEA services have not yet emerged, several requirements examples can improve the state of practice.
		• While EMAs do not always specify them in their requests for proposals (RFPs), some common quality attribute requirements for WEA services have emerged.
			• Spend the time to identify the key requirements, and specify them meaningfully. These requirements include
			  • what the system must do (functional requirements)
			  • how the system must operate (quality attribute requirements)

6	Cloud trends	• EMAs are moving toward public and private cloud-hosted software as a service (SaaS). • EMAs make assumptions about the quality of service (QoS) provided by cloud-vendor products without understanding the key tradeoffs of the vendor's technical strategy.	• Know what QoS you need, and ask how the vendor will achieve it. • Know how to look beyond the jargon and hype.

Section	WEA Topic	Observations	Recommendations
7	Cybersecurity	• Most organizations do not possess a concrete and comprehensive awareness of the cybersecurity risks that they face daily.	• Learn about the security risks associated with modern alerting technologies and establish a culture of good security. • Implement a cybersecurity risk-management strategy.
8	Product selection	• Product selection is becoming more complex. • EMAs may select product features without sufficient consideration of organizational expectations. • There is a tendency to overlook possible consequences of tradeoffs across features and quality attributes, rather than analyzing and factoring them into selection decisions up front.	• Confirm WEA capabilities before purchasing the product. • Develop a customized prioritization method that documents the progression from operational expectations to prioritized features. • EMAs that lead tradeoff discussions should acquire sufficient knowledge of tradeoff definitions and consequences to lead these design discussions. • Fill the role of a “lead integrator” if you will use multiple vendor products.
9	Testing	• There is a lack of understanding about what IPAWS environments are available for testing the WEA service. • EMAs are uncertain about the types of software and system tests that they should conduct.	• Attend FEMA IPAWS webinars and outreach sessions. • Conduct periodic tests of the individual system and software to include interface testing between the alerting software and IPAWS-OPEN using available testing platforms. • Periodically conduct end-to-end testing using available testing platforms.
10	Operations	• Many organizations lack a method for identifying the operational impacts of WEA adoption. • EMAs recognize the need to address and manage operational challenges prior to an emergency incident. • Good practices can assist in sending rapid, clear, and timely messages during an emergency. • Large-scale exercises and training are important to exercise cross-agency and cross-system scenarios. • There are cross-organization coordination challenges in issuing WEA messages. • There are challenges in synchronizing WEA information with other media channels.	• Determine how to manage operational challenges before an emergency event occurs. • Prepare the public to respond appropriately to WEA messages. • Continue learning about alerting capabilities as technology evolves. • Perform interagency training and drilling to plan for coordinating across jurisdictions during an emergency. • Use scenarios and RACI (responsible, accountable, consulted, and informed) sessions to coordinate WEA messaging across organizations. • Work with other EMAs, the media, and the public to synchronize WEA information with other media channels.

11	Alternatives to buying a WEA solution	• EMAs have several options for obtaining a WEA solution, and they each have advantages and disadvantages.
		• There are special considerations for developing your own WEA solution.
		• There are important considerations related to authentication and message validation.
		• There are challenges with error-handling message propagation.
			• Understand the advantages and disadvantages of each build-your-own option so that you can make an informed choice.
			• If you choose to build in-house, then
			  • conduct development and testing in an isolated environment
			  • consider system performance, security, and availability
			  • pay attention to authentication, message validation, and error handling

The report concludes with a brief summary and a discussion of some future considerations. Several appendices provide supplemental information on the research approach and method of data collection; a step-by-step framework for WEA adoption; further discussion of testing considerations, illustrated with an example; examples of an evolutionary path for WEA requirements; and a list of useful resources.

2 The Current State of WEA: Adoption-Related Strengths and Challenges

During our engagements with stakeholders, we observed a number of recurring themes related to the current capabilities of WEA. EMAs have a strong desire to leverage mobile devices as a public alerting mechanism. However, many organizations are struggling with whether to adopt WEA messaging capability. We summarize in this set of observations some of the perceived strengths and weaknesses that we gathered through interviews with EMA stakeholders. This information was derived from our interview data; therefore, the contents of these observations do not necessarily reflect the opinions of the study authors in all cases.

2.1 Observations

Our interactions with EMA stakeholders resulted in two broad observations:

1. WEA has several recognized strengths that make adoption attractive to EMAs.
2. The EMA community has a number of common concerns about WEA, and addressing them would speed adoption.

Observation 1: WEA has several recognized strengths that make adoption attractive to EMAs.

We found that most large counties were actively working to implement a WEA capability. All sampled stakeholders enthusiastically welcomed the addition of WEA to the EMA's toolbox. Many EMA stakeholders emphasized that they plan to use the WEA service as an additional tool, rather than as a replacement for existing solutions. AOs indicated that being able to reach cell phones without a subscription-based service provides a strong business and mission case for the capability. A number of strengths make WEA attractive to EMAs: broad geographic reach, targeting of mobile devices, low cost to the public, high performance, and broad public reach.

Broad reach. Many EMAs are organized around county boundaries. WEA uses cell broadcast, which dispatches alerts using Federal Information Processing Standard (FIPS) codes. This approach provides a convenient way to reach the entire jurisdiction. WEA's county-level targeting capability may reduce its frequency of expected use (discussed in Observation 2); however, WEA's ability to reach large numbers of people quickly in an emergency event is a huge benefit. The WEA service is able to reach people wherever and whenever they have their WEA-capable cell phones turned on. By late 2014, most mobile devices will be WEA-capable devices [FEMA 2012c]. Furthermore, commercial mobile service providers (CMSPs) will preconfigure WEA-capable handsets to receive WEA messages. Users must manually opt out of the service if they do not wish to receive the messages (users cannot opt out of Presidential Alerts) [FCC 2013].

Targeting mobile devices. WEA fulfills a critical need. As of December 2012, more than 35% of residents no longer have landlines, and virtually everyone in the country has a cell phone [Santana 2013]. The cell phone is the most available medium for direct contact with the population. The United States is a mobile society, with tourists and daytime workers swelling populations on a daily basis. WEA messages can reach these transients. Additionally, the subscriber sign-up rates for opt-in services such as Short Message Service–Point-to-Point (SMS-PP) have shown marginal

ability to gain significant subscription rates. For example, New York City's subscriber base of 100,000 people for its opt-in service, called Notify NYC, reaches only a small fraction of the city's 8 million residents and 49 million annual visitors [Trocki Stark 2013]. While people can opt out of WEA for Imminent Threat and AMBER Alerts, they do not need to opt in. All WEA-capable cell phones will receive WEA messages automatically, so the service will reach many more phones. Thus, WEA is critical for reaching the public in times of emergency.

Low cost. The carriers are not permitted to charge end users for the service. FEMA provides a set of free software objects that developers can use to build message-generation capabilities, and many vendors of products used with EAS are now working to provide WEA messaging capabilities as part of their product suites.

High performance. Organizations, such as the NWS, are actively issuing WEA messages. The NWS reports that the system is very responsive, with messages reaching handsets within seconds of being presented to IPAWS. A strength is the use of SMS–Cell Broadcast (SMS-CB), a one-to-many service, which simultaneously delivers messages to multiple recipients in a specified area. Using SMS-CB as the delivery technology avoids the congestion issues currently experienced by traditional SMS-PP approaches, which directly translates into faster delivery of messages during times of emergency [IdeaScale 2012].

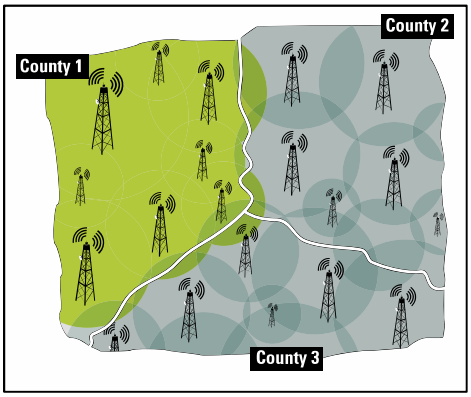
Observation 2: The EMA community has a number of common concerns about WEA, and addressing them would speed adoption.

Stakeholders have a number of common concerns about WEA, according to results of our interviews. Some of these concerns are inherent in the current implementation of WEA. However, many of the concerns are not systemic, so there is reasonable hope for medium- and short-term solutions. In some cases, EMAs cannot do anything about the concerns and will simply need to wait for WEA standards and the carriers' services to evolve. This report includes such concerns for awareness and not action. These concerns include geotargeting granularity and message bleed-over beyond the targeted area, the 90-character message limit, carrier coverage, older handsets, addressing individual needs, trust, opting out, resource limitations, determining vendor compliance, and cross-jurisdictional issues.

Finer granularity and less bleed-over. The granularity of message coverage is a known challenge for the WEA service. Interviewees reported that the current governing standards were derived based on large-scale incidents, such as a nuclear attack, for which EMAs would expect to notify multiple counties. This design decision produced a coverage granularity at the county level, facilitated by FIPS codes [for more information, see NIST 2013]. The CAP standards allow for the specification of a coverage polygon, which could be larger or smaller than the county, to be defined [FEMA 2013c]. According to an author of the CAP standard, the original intent of CAP was that where both polygon and FIPS elements are populated, the more precise geometries (polygons and circle) would be preferred over geocodes (e.g., FIPS codes). However, the OASIS standard language does not dictate how FEMA will process and use the elements. FEMA could send the message using either populated element (polygon or FIPS) or both elements. Giving preference to explicit geometries, such as polygons, when they are provided should enable more precise delivery.

Especially in western states where counties are large, EMAs do not want to issue WEA messages that blanket their large counties because the messages will go to people beyond those in the impacted area. “Some of our counties are bigger than entire states back East” is a repeated sentiment from the Midwest to the West Coast. They anticipate that this over-warning will cause some cell phone users to opt out of WEA and thus miss receiving messages that do affect them. As a result, some larger western EMAs report that they will not use the WEA service for this reason. This is not as big an issue on the East Coast, where counties are smaller, although EMAs in this area still would prefer finer granularity.

Figure 2 illustrates how overlapping cell tower coverage may cause another type of over-warning called *bleed-over*. EMAs confirm that an effect of bleed-over is duplication and potentially conflicting alerts. For instance, in this diagram, if County 1 issues an evacuation order while County 3 issues a shelter-in-place order, people in the bleed-over area along the county borders may receive both messages.



Some encouraging developments indicate that a resolution of these concerns may be near. At a National Academy of Science Workshop on Geotargeted Alerts and Warnings on February 22, 2013, FEMA reported that the four largest carriers now allow the polygon definition to take priority over the FIPS code [NAS 2013]. For the future, OASIS committee members report that the next version of CAP will codify this priority adjustment.

The 90-character message limit. One comment we heard frequently from stakeholders is that they perceived the 90-character limit to be a significant limitation of the WEA service. While this could be a limiting factor, we suggest two responses to this:

1. *In many cases, 90 characters are enough.* We suggest that perception may not reflect reality in some cases if EMAs use the WEA service as intended. Many interviewees reported that the length appears to be sufficient to act as the “bell ringer” during an event; they likened the limitation to that of highway sign boards or television alerting “crawls.” The WEA service is not intended to be the sole information distribution channel. EMAs should use other sources such as local alerting or media outlets to provide more detailed location-specific instructions for citizens to follow in the event of an emergency.
2. *Sequences of CMAM text may be an option.* At the National Academy of Sciences meeting in February 2013, one of the vendor representatives suggested that a longer message could be created using a series of shorter messages to improve alerting effectiveness [NAS 2013]. The

CMAM text field (also restricted to 90 characters) of the IPAWS-OPEN CAP Profile can be used to create the individual messages in the series of sequenced messages.

Carrier coverage. Carriers may not provide coverage for parts of the United States.[3] Carriers report that they consider demographics and system capability data as confidential information. EMAs report that they do not have a ready source of tower coverage or information about handset capabilities in their jurisdictions, so it is difficult to predict how many people would receive a WEA message in a given area.

Not all handsets are WEA-capable handsets. It is not uncommon for an alert to be delivered to one phone but not to another because not all phones are currently WEA-capable phones. It is expected that by late 2014, most new mobile devices will be WEA-capable devices [FEMA 2012c]. The FCC requires all wireless carriers that do not participate in WEA to notify their customers [FCC 2013]. For more information on WEA-capable devices and carrier coverage, see "Device Information" in Appendix G: Resources.

Addressing individual needs. Interviewees reported that the WEA service does not address individual needs of various population segments at all the specification levels. For example, the CAP supports multiple languages, but the category and response descriptors for WEA are defined only in English [FEMA 2013c[4]]. The handset manufacturers provide some capabilities that address individual needs. For example, one of the major carriers indicated that it has phones with features such as font resizing for the vision impaired, text-to-voice translation for the blind, and vibration annunciation of the ring tone for the deaf available on some handsets.

Trust. One of the repeated statements from the stakeholders we interviewed was that the public should be educated about WEA messaging, and individual, city, county, and state levels need to focus on public outreach to avoid confusing the people and to generate trust in the messages. The public needs to be informed about the public-facing aspects of the message protocols. For example, the National Weather Service tags its messages with "NWS." It might take time for the public to recognize and trust this identifier.

Opting out. Many interviewees expressed concern that circumstances such as false alerts, poorly targeted alerts, or alerts that do not concern the receivers will cause people to opt out of the service. Once they leave, the interviewees worried, it will be difficult to get them to come back. Experience will tell the degree to which this concern may be realized.

Limited EMA resources. Authorities in smaller localities might not adopt WEA capabilities because of staff and budget limitations. One mitigation suggested by several stakeholders is "in the name of" alerting, in which a small organization finds a trusted partner with a WEA messaging solution that would issue alerts on behalf of the smaller organization. For example, the NWS has a history of assisting local authorities with other types of alerting.

---

[3] For example, as of April 2013 only half of the land base of the Navajo Nation had wireless coverage, and only 37% of the population had cell phones [Landry 2013]. Landry writes, "The Navajo phrase for cell phone is 'bil n'joobal',' or 'something you use while spinning around in circles.' The phrase is based on the description of someone spinning around with a phone, trying to get good reception."

[4] FEMA provides this guide to those who execute the developer MOA.

Determining vendor IPAWS compliance. It can be difficult to determine whether vendors' products support IPAWS. Section 8 covers this concern in more detail.

Cross-jurisdictional issues. EMAs will need to coordinate among adjacent jurisdictions to mutually agree on protocols to minimize the negative impacts of bleed-over as well as address cross-media coordination. Section 10 covers this concern in more detail.

2.2 Summary

Of all the adoption barriers identified, interview participants cited the geotargeting granularity and the 90-character limit most frequently as significant impediments. DHS is actively researching these areas, and carriers appear to be moving toward the polygon-mapping approach for coverage broadcast. The standards community supports steps to implement polygon-based geotargeting, and the carriers predict that the move to 4G long-term evolution (LTE) protocols will reduce bleed-over significantly.

The alert-originator community could mitigate the 90-character limit with public education and outreach. As people learn that WEA messages are bell ringers that provide more information than sirens, they will also learn where to seek more detailed information from other sources. Additionally, at least one CMSP has suggested that, in the future, linked, consecutive messages could provide much longer messaging capabilities. We assume this would have some ripple effects on the handsets and message-origination software, but it would have little impact on the transport infrastructure.

Another significant challenge area is EMAs' resources for establishing WEA-capable solutions. Resource challenges are universal, but the high value of WEA messages during an emergency could motivate "in the name of" alerting partnerships as a viable mitigation to the cost of WEA adoption. For those who do not have a budget to implement their own WEA-capable solutions, organizations such as the National Emergency Management Agency could offer to send alerts on behalf of neighboring communities when appropriate. In addition, the International Association of Emergency Managers could help establish strategic partnerships with other Collaborative Operating Groups (COGs) who have established alerting programs.

In conclusion, this compilation of observations comes from many forward-looking early adopters of WEA. Real-world experience may change initial attitudes and beliefs. Additional research to calibrate initial perceptions against objective observations and to track evolving WEA maturity could provide benefits for development efforts.

3 Integrated WEA: Another Important Tool in the EMA Toolbox

In this section, we summarize the point that EMAs do not view WEA as a stand-alone capability; rather, they look at WEA as part of an integrated set of tools. This observation is consistent with FEMA's position that the WEA service is not intended to replace established alerting tools or communication pathways by which AOs currently warn the public of an emergency event. It is intended to provide additional capability. Thus, EMAs can adapt the WEA adoption considerations in this report to build a strategy appropriate to their organizations. This is important for setting the context of this report because while our focus is on EMA alert origination and integration, we also cover a variety of related topics.

3.1 Observation

Observation: EMAs consider WEA as an augmentation to their suite of alerting tools, not as a stand-alone system.

EMAs quickly made clear that it makes no sense to them to talk about WEA as a stand-alone capability. Rather, EMAs suggested looking at the whole picture of WEA usage—how WEA is used and integrated with other EMA tools—to meet user needs. This is an important point because, although we focused on WEA, our observations naturally cross boundaries into integration with other tools and related topics. This observation makes clear that understanding the context in which an EMA will use WEA holds the key to the complexity and integration challenges. Figure 3, from the vendor Alerting Solutions, illustrates how complex a context can be.

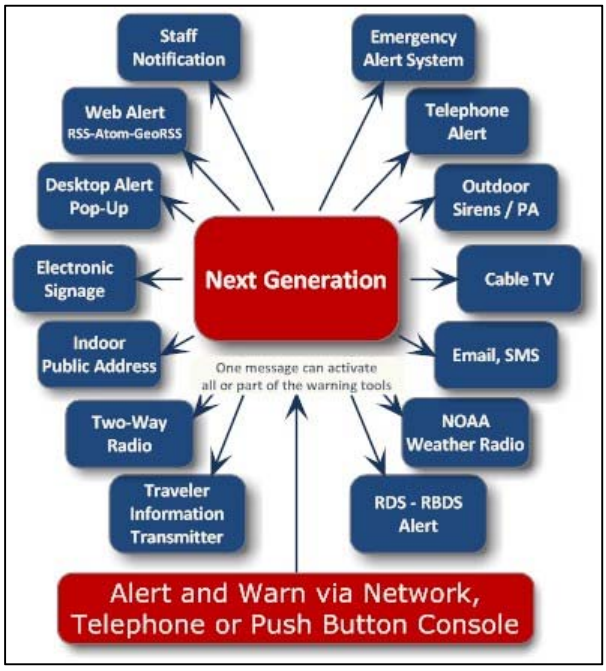


Figure 3: Tools for Communicating Alerts and Warnings [© Alerting Solutions, Inc. Reprinted from Alerting Solutions 2013]

Throughout stakeholder interviews, EMAs expressed the need for "seamless, easy-to-use, integrated" solutions during emergency situations (e.g., they want one solution for both emergency management and mass alerting). In practice, EMAs are implementing a range of WEA tool-integration strategies from completely stand-alone (least desirable) to fully integrated (most desirable).

The scope of this study included WEA integration through emergency-warning solutions as well as related topics such as emergency-management solutions, situational-awareness solutions, and social-media websites.

3.2 Recommendation

Consider WEA adoption from an integrated perspective.

Rather than considering the WEA service as a separate tool, look at it as another tool to integrate into the technology solution suite in support of emergency management. We suggest that EMAs carefully consider where WEA fits into their overall technical integration strategy as well as overarching emergency management goals. This integrated perspective will help EMAs better articulate their needs in terms of technical requirements, evaluate and select products to support alerting, integrate alerting solutions with other solutions (avoiding redundancy), and maintain the alerting solution throughout its life cycle. In this document, we focus on considerations that EMAs should be aware of as they proceed with WEA service adoption.

4 Integration Strategy Considerations

In the previous section, we discussed the observation that EMAs do not view WEA adoption in isolation. For EMAs, WEA is part of a bigger vision and context. In this section, we discuss some examples of the challenges that EMAs face as they move toward a future vision for emergency management. We draw our observations in this section from three cases studies, interviews with EMAs, and examples from recent emergency incidents. Collectively, these examples illustrate the growing complexity that EMAs face as they move toward a more technically and organizationally integrated emergency-management environment.

A key observation from our analysis is that today's task of emergency management and warning involves orchestrating many loosely coupled systems managed by different organizations. These types of systems of systems present many technical and operational challenges [Gagliardi 2010, SEI 2009]. EMAs are just beginning to understand these new challenges, and many have little experience with systems analysis at this scale. Certainly, the EMA community is very technically savvy. However, most EMA staff were not hired to plan for and integrate large-scale, loosely coupled systems of systems.

To be clear, adding WEA to EMAs' toolboxes has not created this complexity. Rather, the complexity is part of the natural extension of the increasingly complex communications infrastructure of modern society.

4.1 Observations

Within this context, engagements with stakeholders exposed two broad observations:

1. The need to integrate a variety of technologies and methods to reach the public (e.g., alerting solutions, website, call centers) has increased the need for more rigor in integration design and analysis.
2. As both the scale of emergency management systems and EMAs' responsibility increases, integration complexity increases.

Observation 1: The need to integrate a variety of technologies and methods to reach the public (e.g., alerting solutions, website, call centers) has increased the need for more rigor in integration design and analysis.

Through examples captured during interviews with EMAs, we observed that they are dealing with a variety of new challenges as they grapple with the technologies and channels available to them. They struggle with how to keep up with current technology and put together a technology strategy that is attainable within budget but forward looking enough that it is not soon obsolete. At the same time, EMAs need to reason about supporting cross-organizational systems. This involves integration issues that are outside their boundary of control. Our experience with similar systems tells us that this requires an understanding for how people and systems interact well beyond sending a WEA message. While it is critical to get people out of harm's way, we have learned that it is also critical to have resilient and accessible telecommunication and information systems in place for people to get more information.

A recurring theme for EMAs is the saturation of commercial cellular voice and data channels during an emergency. For example, shortly after the Boston Marathon bombing, *The Boston Globe* described the problem:

> *Widespread problems with cellphone service around Boston on Monday after the Marathon bombings put the limits of the nation's wireless network into sharp relief, as the nation's top carriers were unable to cope under the heaviest loads during the most crucial moments.*
>
> *Verizon Wireless, AT&T, and Sprint were all overwhelmed by the surge in traffic, leaving many at the scene of the explosions unable to contact family or friends, and blocked other callers in the area or outside Boston from checking on those attending the Marathon. [Farrell 2013]*

Carrier networks do not function well during times of saturation, which can limit the public's ability to use cell phones to make calls. Wi-Fi availability is becoming increasingly prominent, particularly within large cities. Wi-Fi-accessible hyperlinks within the WEA message could lighten the load on the networks. For example, rather than overloading voice and data cellular networks with cell phone calls and searches for more information over the cell-data network, people could access more detailed information over the Wi-Fi channel (if one is available). At the time of writing, URLs were not permitted in WEA messages (although the CAP standard does support them). Consequently, WEA message recipients make lengthy phone calls during emergencies, locking up the carrier networks. Note that this problem is not caused by WEA but illustrates how WEA fits into the larger picture of emergency alerting systems. The point here is that WEA cannot be viewed in strict isolation.

We provide a second example that illustrates the need to think broadly about integration (shown in Figure 4). This example is based on a scenario discussed during the Mission Thread Workshop sessions that we conducted with emergency-management offices (described in Section 10). The steps in Figure 4 are described as follows:

1a. A hazardous spill event occurs. The EMA determines that the event warrants a WEA message to be issued.

1b. The WEA message is crafted using the EMA's emergency notification system (ENS). The ENS sends the WEA message to the IPAWS Alert Aggregator.

2. IPAW Alert Aggregator communicates to the CMSPs, which distribute the message through cell towers in the geographically targeted area.

3. Citizens receive the WEA message and seek additional information about the event by calling 911 (inappropriately) and visiting the community emergency-management website. The 911 phone lines are busy, and the website is flooded with requests, so citizens cannot obtain additional information.

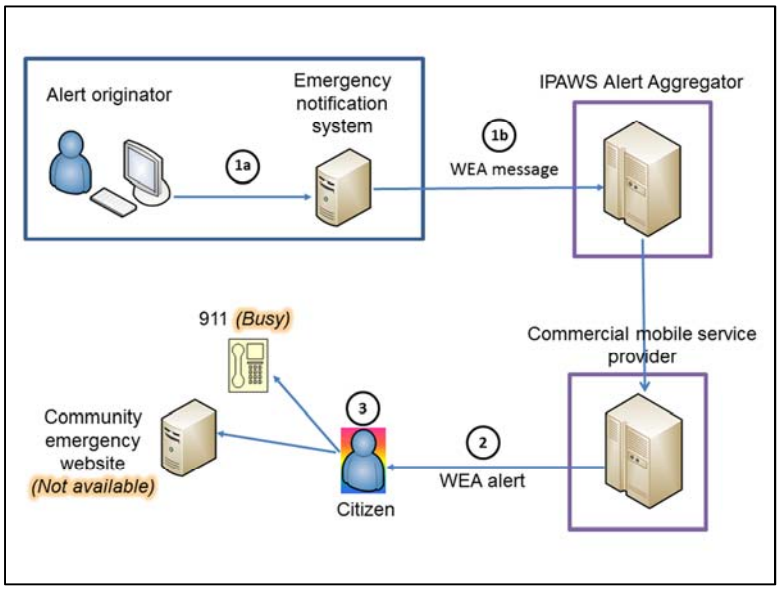


Figure 4: An Emergency Triggers 911 and Website Flooding

The problem is not limited to cell phone saturation; it also affects access to data networks. Some carriers are already struggling to keep up. Philip Cusick, an analyst at Macquarie Securities, has noted, "Carrier networks aren't set to handle 5 million tablets sucking down 5 gigabytes of data each month" [Wortham 2010].

What can EMAs do? We suggest that analyzing scenarios such as these, which go beyond the scope of WEA message dissemination, can help EMAs identify potential bottlenecks and help them think about mitigation options. For example, although EMAs have no control over carrier capacity during emergency situations, they can consider possible mitigation options. Options may include directing people to try using Wi-Fi hotspots during emergencies to make calls over the internet (e.g., VoIP) or to a website capable of scaling to the level needed during an emergency (which, of course, requires additional technical analysis). Obviously, there are tradeoffs with these options, and these are suggestions, not directives. We provide them to illustrate the importance of end-to-end systems analysis. End-to-end and large-scale systems require systems analysis considerations throughout all stages of product acquisition, operations, and sustainment. We provide some suggestions for life-cycle analysis considerations in the recommendations at the end of this section.

Observation 2: As both the scale of emergency management systems and EMAs' responsiblity increase, integration complexity increases.

In this section, we summarize and analyze three cases studies. The key finding is that as emergency-management systems increase in scale and responsibility to reach large populations, integration complexity also increases. This is a particular concern for larger jurisdictions such as heavily populated counties or states. The case studies in this section represent examples from three real organizational levels: (1) an individual local EMA, in Case Study A; (2) a county-level EMA, in Case Study B; and (3) a state-level EMA, in Case Study C. These examples illustrate some of challenges that EMAs face.

Case Study Summary A: Individual (Local) EMA

Organization A has a small staff that includes an emergency-management director. Staff members receive emergency information from the sheriff's office, first responders, and a 911 center. The EMA was the first organization in its state to be certified to send WEA messages. It helped drive the state to determine the policies and procedures for WEA approval. Because the EMA staff could not find comparable examples in their own state, they collaborated with another state to develop their emergency-management integration approach.

Figure 5 illustrates the current configuration for this EMA. The EMA staff uses a subscription-based solution, CodeRed, to send alerts via email, phone calls, and text messages. They leverage a software product called EMnet to send EAS and WEA messages to the IPAWS Aggregator. They use a software product called WebEOC for incident management. Currently, they must be on-site to use EMnet. To improve response time in an emergency, this EMA created alert templates and sample messages. The EMA has a satellite backup capability in case it loses internet access as well as redundant fiber-optic cables for the internet connection. In the future, they would like to have remote access to EMnet and to target WEA messages within a two-mile radius.

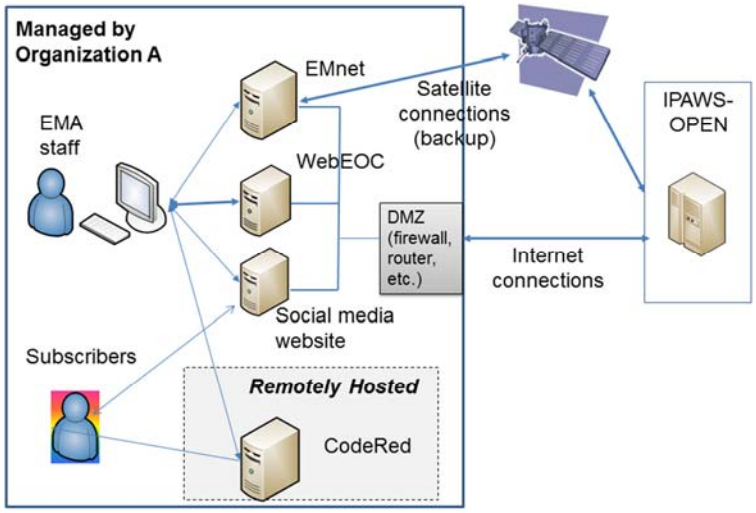


Figure 5: Case Study A – Individual EMA

Case Study Summary B: County-Level EMA

This EMA serves one of the largest population centers in the United States. It spans 34 cities and 125 law enforcement jurisdictions. It is staffed by multiple operators who originate alerts, an IT representative, first responders, and an on-site state EMA representative. The EMA receives emergency information from firefighters, police, other in-state EMAs, the state EMA, FEMA, the 911 center, television stations, and an entity that provides ocean shipping information. The EMA is currently the lead coordinator for communication between the state and federal entities such as FEMA. The EMA staff members are also developing a warning severity scale to determine which alert channels are appropriate for different incidents.

Figure 6 illustrates the current configuration of this EMA. Staff members use a software product called Nixle to generate WEA messages. They use WebEOC for incident management, developed their own situational-analysis application, and use a warning and notification system provided by the state that does not yet have WEA capability. They are investigating other solutions to make their system more integrated. The WebEOC server is backed up at the vendor site to provide redundancy and site continuity. The on-site server that hosts the situational-awareness application also has site continuity provisions. The EMA has 100% back-up power capability and a highly redundant data architecture.

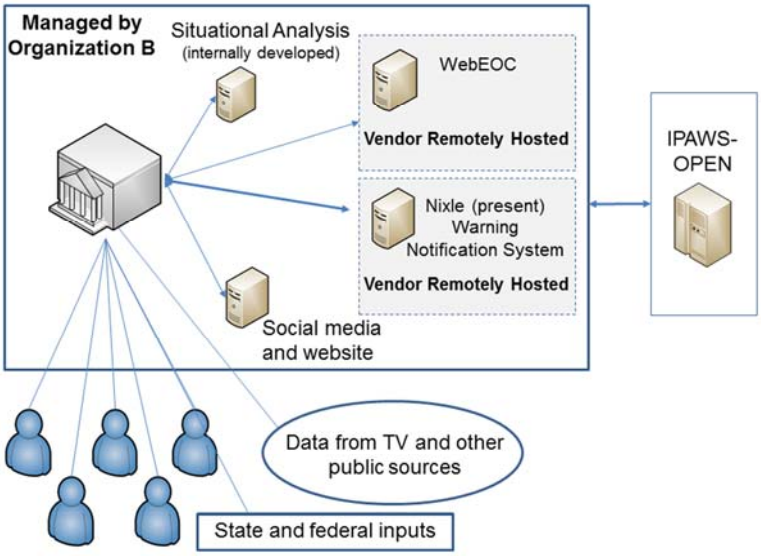


Figure 6: Case Study B – County-Level EMA

Case Study Summary C: State EMA

The EMA is staffed by 28 full-time people, including emergency managers and IT personnel. This state EMA has roles and responsibilities significantly different from individual and county EMAs. The state EMA staff members receive emergency information from federal agencies and provide emergency notification to subscribers via Emergency Notification phone alerts, television, website, and social media. They also fill gaps in EMA coverage in the state. This EMA guides individual and county EMAs in the state and certifies EMAs for WEA. Staff members are developing an emergency-management strategy that integrates in-state EMAs, universities, and other agencies into the WEA service and enables these subsidiary organizations to issue WEA messages locally. However, this state EMA would like to maintain broad control of all outgoing emergency information for consistency.

Figure 7 illustrates the current configuration for this state EMA. The EMA grants in-state EMAs permission to use the statewide WebEOC license. It also has a subscription system for residents called GovDelivery, which interfaces with the web-management solution. The EMA wants to transition their legacy system to a new system that integrates with WEA so that when originators issue an alert, it will be sent to the IPAWS Aggregator and to GovDelivery simultaneously. Staff members are also investigating a map-based situational-analysis solution. The EMA is exploring multiple paths to transmit messages to improve availability, including sending messages via public radio through the state public broadcasting system.

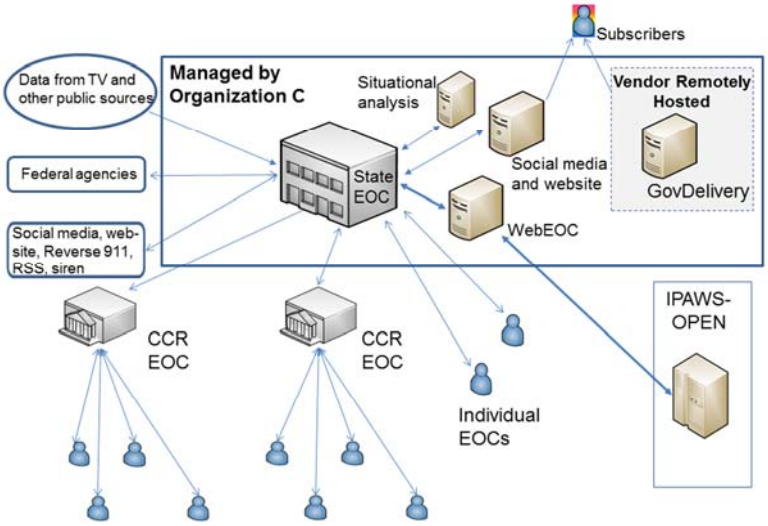


Figure 7: Case Study C – State-Level EMA

Using the case study data as a backdrop, we summarize our observations here. The case studies indicate increasing integration complexity as organization size and responsibilities expand (shown in Figure 8). We also found that states expect individual and county EMAs to take on more responsibility, which can mean that the technical risks increase and the need for systems-integration design increases. For example, emergency-management integration strategies that started as tool-picking projects often become full-scale integration projects at the larger organization levels. These EMAs should consider an integration strategy for their emergency-management solutions in order to serve large internal and external communities. They should also apply more rigor to design and integration as they consider information flow across a greater variety of systems and information channels. However, often EMAs were not aware that in choosing a WEA-capable product they were also making system or software engineering decisions that may have far-reaching effects. As technical risks and the engineering complexity increase, ad hoc tool acquisition and system-design strategies start to reach their limits.

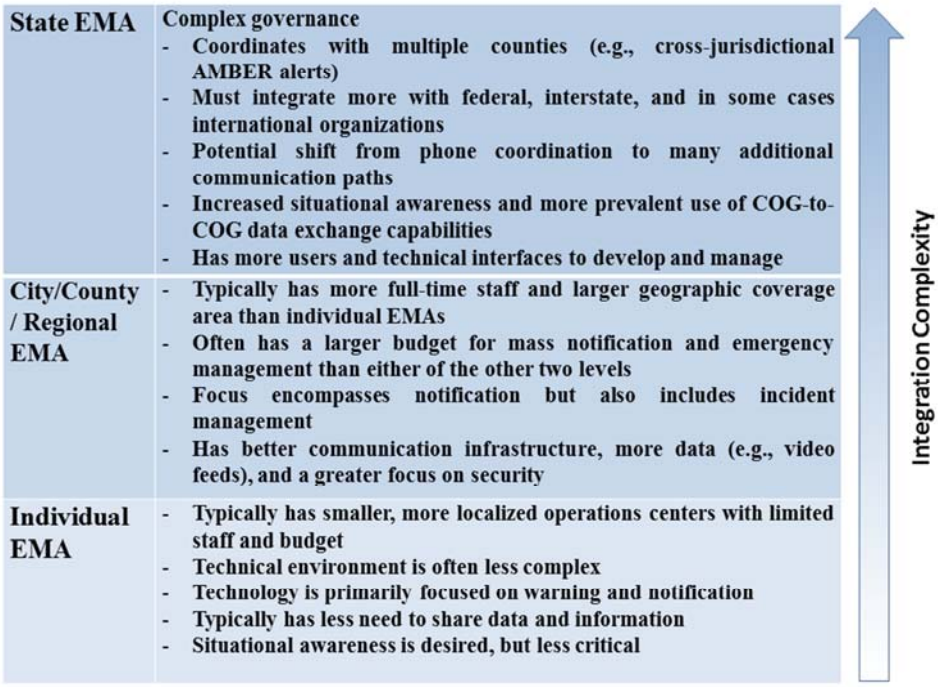


Figure 8: Summary of Organizational Characteristics Derived from Case Studies

4.2 Recommendation

Focus on "bigger picture" system analysis throughout the integration-strategy life cycle.

As opportunities afforded by modern emergency-management technology (including WEA) increase, so do integration complexity and alerting responsibility. To use the new technology effectively to reach the public, EMAs should consider technical scenarios often outside their areas of technical expertise. They are beginning to realize that they need to consider a bigger picture and longer term implications of what used to be rather simple, isolated decisions such as product selection. EMAs that have not considered systems engineering as part of their role now find themselves having to make systems-engineering decisions. Design and planning in the early stages of technology adoption can prevent many problems later. This section provides some suggestions for integrating big-picture systems at different stages during the integrated-solution acquisition and management life cycle.

Planning for the future of alerting and emergency warning. We make two suggestions for the planning phase:

1. Focus on strategic planning for future iterations of emergency management and alerting systems.
2. Analyze current scenarios to understand areas of potential fault and failure.

Strategic planning considerations should include defining business and mission goals and determining the technical integration strategy to support those goals. We also suggest developing some forward-looking, end-to-end emergency scenarios with a heavy focus on areas where there could be system-capacity bottlenecks, single points of failure, or gaps in information flow. One method

for this type of analysis is the Mission Thread Workshop, described in Section 10 and Appendix B of this report.

Requirements. Requirements should include support for end-to-end scenarios and clearly specify the EMA's scalability, performance, and availability needs (see Section 5 for more information on requirements).

Analysis and design. Few EMAs had any type of enterprise view for their emergency-management integration design or architecture; however, several conveyed the need for this. We suggest that EMAs document at least a high-level view of their technology landscape so that they can understand the implications of adding new solutions to the existing infrastructure. This documentation is also a useful artifact to have for the analysis of emergency scenarios. Another important consideration for EMAs is the potential need for integration software. If an EMA buys a variety of disparate products but desires a seamless interface, design and maintenance are required to integrate multiple software products. We suggest that this is an area where EMAs will want to focus particular attention to design and maintenance tradeoffs.

Implementation. Most EMAs will not build their own systems. For those that do, Section 11 contains considerations for those organizations exploring the "build it" option.

Testing, evaluation, and sustainment. Complex systems need regular testing to provide confidence that they will perform when needed. Section 9 provides more information about testing considerations.

In conclusion, to deal with increasing integration opportunity and complexity, EMAs will need to change their mindset from adopting products and technologies separately (such as WEA) to thinking of solution integration from the perspective of big-picture systems integration. This requires thinking about the impact of decisions on integration strategy throughout each stage of the product purchase or development life cycle as they adopt new technology capabilities.

5 Requirements Considerations

Requirements are statements of what a system must do, how it must behave, the properties it must exhibit, the qualities it must possess, and the constraints that the system must satisfy [Bass 2012]. Because EMAs communicate their needs to vendors (or developers, for those building their own systems) through requirements, clear and accurate requirement statements are key to acquiring systems that meet an EMA's mission needs.

The investigation into EMA requirements-specification practices included data collection from interviews with EMAs, analysis of RFP documentation, conference attendance, visits to EMA work sites, and other stakeholder interaction. The data-collection effort and subsequent analysis resulted in three observations:

1. EMAs struggle with specifying complete and unambiguous requirements in their RFPs.
2. While functional requirements for WEA services are to some degree context specific, we provide several requirements examples that can improve the state of practice.
3. While EMAs do not always specify them in their RFPs, some common quality attribute requirements for WEA services have emerged.

Before we present the observations and recommendations, we define some key terms for requirements.

5.1 Defining Terms

Technical system requirements may be classified into the following categories[5] [Bass 2012], which Figure 9 illustrates:

- **Functional requirements.** These requirements specify what the system must do and how it must behave or react during operations. Functional requirements can be described as user stories; for example, "The user clicks *this* button and the system retrieves *that* data and displays it on a screen."
- **Non-functional (quality attribute) requirements.** Quality attribute requirements, often referred to as non-functional requirements, communicate qualities or properties that users expect the system to support. These requirements typically add qualifications to the functional requirements or to the overall system. A quality attribute requirement might specify how fast the system must perform the function or how resilient the system must be in the face of erroneous inputs. These requirements are often called the "-ilities"—such as availability, scalability, reliability, usability, maintainability, and testability. An example of a quality attribute applied to the earlier functional example could be "The user clicks *this* button and the system retrieves *that* data and displays it on a screen *within this many seconds.*" The time specification is the quality attribute requirement.

  It is important to properly specify quality attribute requirements because they typically have considerable design implications. For example, EMAs often said they planned to strengthen

[5] Those developing their own systems also are subject to a third type of requirement: *constraints*.

security later, after the system is in place; however, adding security features after selecting or developing the system is much more difficult than adding them earlier [Bass 2012].

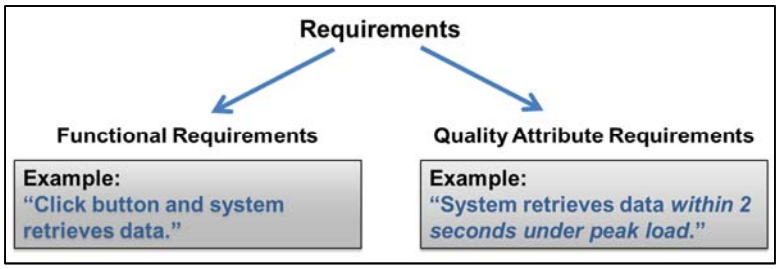


Figure 9: Categories of Requirements

Non-technical requirements. Non-technical requirements relate to customer-support activities, such as help-line availability, on-site support, or responsiveness to system problems, and licensing details, such as cost based on the number of users. While these are important considerations, EMAs should specify and evaluate non-technical requirements separately from technical requirements. This separation of concerns will make it easier to evaluate competing solutions. Furthermore, technical requirements are useful artifacts that EMAs can employ later in the implementation life cycle to develop system and software test cases, so it is important to have a clearly specified and thorough set of technical requirements that describes what the system should do and how well it should do it (e.g., in terms of performance, security, and availability).

This background information will help explain common challenges in specifying WEA product requirements and the guidance to improve both functional and quality attribute requirements specifications in RFPs.

5.2 Observations

Observation 1: EMAs struggle with communicating their requirements to vendors.

Data analysis revealed that many EMAs struggle to specify their requirements. This results in difficulty in communicating the EMA's true needs to potential suppliers, evaluating competing proposals, and determining whether a delivered system meets the actual needs.

First, the RFPs showed a mixing of functional, non-functional, and non-technical requirements as well as business goals. That makes it difficult to locate the technical requirement specifications that are key for complete and accurate evaluation of technical products. Moreover, some of the requirements we found during RFP review read like technical requirements but actually are not. For example, one technical requirement specified "24/7 technical support." This is actually a human-resource support requirement, which is important but should not be mixed with the technical requirements against which the EMA will evaluate the delivered system. Another RFP included the requirement to "Obtain the most reliable, economical, and effective approach to alert the public of community emergencies." This is an example of a mission goal that pertains to the operation of the system as well as the procurement itself. This requirement would be very difficult for vendors to bid for or develop, and the vendor response probably would not be very enlightening ("Of course we can do this!").

Second, several of the requirements within the RFPs fall short of best practices for requirements specification. Good requirements are unambiguous, are measureable (and thus testable), specify a need but avoid specifying a solution, and include all important necessities.

In our review, we found several instances of ambiguous or vague requirements. Such specifications often contained unstated assumptions. Examples include requirements for a "user-friendly web interface" or "true SMS technology." Vague requirements are difficult to measure or evaluate. Requirements must be specific enough that vendors can respond to them and an organization can evaluate against them. Vague requirements may have little bearing on a desired solution that includes WEA.

Lack of measurability is a characteristic of ambiguous requirements. Many of the EMA requirements that we analyzed were not measureable, were unrealistic, or were too costly to implement. For instance, the "ability to initiate messages 24x7" has a quantifiable measure, but it specifies 100% availability. It aims for perfection, which is unrealistic and very expensive. A requirement for "99.9% availability" would be a measurable way to specify a more realistic requirement.

In several instances, requirements specified design (or strongly suggested design) rather than need. For example, "vendor must have geographically dispersed data centers" dictates that the vendor should have a distributed infrastructure design, but it is unclear what goal this is expected to achieve. We might assume that the EMA intends the requirement to support availability or reliability, but without knowing the specific need or scenario that the system should meet, neither the EMA nor the vendor can accurately evaluate it.

Regarding completeness of requirements, we found that EMAs specified many functional requirements at only a very high level. For example, a bare-bones functional requirement might be "The system shall be capable of sending WEA messages." This leaves a host of functions unspecified, such as "The system shall provide templates for WEA message composition and modification."

We found it encouraging that EMAs were generally aware of the need to specify quality attribute requirements, but they struggled with how to do this. (See the discussion of Observation 3.) The most common problems were a lack of specificity or measurability. As part of the data analysis, we collected a list of commonly used quality attributes. These are good starting points, but they require more specificity:

- "high-speed" performance
- "high-volume" scalability
- "robust" reliability and availability
- "24/7" availability
- "highly secure" security
- "send to specific radius" configurability
- "redundant" resilience, availability, and failover
- "multiple language delivery options"
- "configurability"

Some requirements that were forgotten more often than others included security, testability, integrability, performance, and modifiability.

Having illustrated typical problems in requirements specifications, we now offer guidance on how to address these problems.

5.2.1 Specifying Functional Requirements

Observation 2: There is a need to better specify functional requirements.

In our RFP analysis, we observed that EMAs described WEA-related functionality only very generally. Some examples include

- ability to define a WEA messaging boundary (even if this gets reset to FIPS code now, the interface should support future improvements)
- ability to send a WEA message to IPAWS-OPEN
- ability to display error messages to system users (and possibly notify the system administrator)
- support for operator message-template creation and modification
- ability to define alerting roles and assign privileges and rules for alerting accordingly

We suggest that further elaboration of functional requirements will better enable EMAs to validate that a proposed solution will meet their needs. Specifying functional requirements for today's needs is a good start, but it is also important to consider how EMA needs might evolve. We suggest that stakeholders consider "exploratory" scenarios to illuminate future needs well beyond what they can envision today. Exploratory scenarios reflect *anticipated* changes to a system [Clements 2002].[6] For example, if a current system specifies geographic coverage through the keyboard entry of a FIPS code, an exploratory scenario might be to replace this operator interface with a graphical interface that allows an operator-controlled polygon to specify the alert area. Another anticipated exploratory scenario might be doubling the number of operators that can simultaneously use the system. An additional example of an exploratory scenario gathered as part of data collection is provided in Appendix F: Example Exploratory Requirements.

5.2.2 Specifying Better Quality Attribute Requirements

Observation 3: While EMAs do not always specify them in their RFPs, some common quality attribute requirements for WEA services have emerged.

As we interviewed stakeholders, we observed several quality attributes that EMA stakeholders said were important. However, these quality attributes were often not included in RFPs and associated documents, and if they were, the specifications were typically vague. Figure 10 illustrates these key quality attributes. In this section, we address how to specify these requirements more precisely and completely.

[6] The reference discusses software architecture evaluation techniques, but the scenario-based approach has been successfully applied to systems and systems of systems.

Figure 10: Key Quality Attributes for a WEA Service

EMAs can improve their specification of quality attributes in two important ways:

1. Specifying the quality attributes in an operationally meaningful and measurable way
2. Specifying key quality attributes

5.2.3 Specifying Quality Attributes in an Operationally Meaningful and Measurable Way

Citing the desired qualities is not enough; it is not useful to say that the system shall be "reliable," "interoperable," or "secure" without details about the context. One-word descriptions for quality attribute requirements do not allow bidders to respond to an RFP confidently or development teams to develop quality designs. A useful check for any requirement is to ask, "Can I come up with a simple test to evaluate whether a proposal (or the delivered system) meets this requirement?" If the answer is "No," then the requirement must be improved. The practice of developing quality attribute scenarios can remove this imprecision and enable EMAs to specify desired qualities and evaluate them meaningfully.[7]

A quality attribute scenario is a short description of an interaction between a stakeholder and a system and the response from the system. A useful quality attribute scenario has three parts:

- **stimulus:** the event that triggers the interaction with the system
- **environment:** the conditions under which the stimulus occurs (e.g., under overload conditions or under normal operations)
- **response:** what the system does in response to the stimulus, including a measurable response for testing the requirement

Here are two short examples of quality attribute scenarios:

[7] Adapted from Bass [2012]. Designers can better guide design by expanding these scenarios to six-part scenarios with the technical detail described in the reference.

- A “performance” scenario: A trained dispatcher is able to construct and send a WEA message under peak system load within one minute.
  - stimulus: trained dispatcher activation
  - environment: peak loading
  - response: The system guides template-driven message creation and sends the message to the IPAWS Aggregator within one minute.

  Note: This performance-oriented scenario is much more specific than “the system shall respond in a timely fashion.”
- An “availability” scenario: A hardware fault causes the primary system to crash during peak load, but users experience no more than 30 seconds of downtime.
  - stimulus: hardware fault
  - environment: peak loading
  - response: The system recovers within 30 seconds.

  Note: This scenario avoids specifying a design solution (e.g., “the system shall cut over to a backup system within 30 seconds” would specify a design solution), but rather specifies the operational need and leaves the implementation to the vendor or designer.

A benefit of specifying measurable and specific criteria is that EMAs can use the specification to evaluate designs for proposal submissions. The detailed scenario makes the requirement clear, so the solution can be evaluated and tested against it.

Not every requirement needs to be specified to this detail. EMAs should focus on specifying in detail the requirements that have high business value and that would be hard to change later. Once the organization gains experience specifying requirements this way, it can represent key quality attributes with a fairly small number of scenarios. A few dozen scenarios can represent even many complex systems.

While functional requirements also require appropriate specification, changes to functional requirements are often less disruptive than changes to quality attribute requirements. For example, improving security or performance after the system is in place is typically an expensive and time-consuming undertaking. It is best to specify these types of requirements in more detail up front.

5.2.4 Specifying Key Quality Attributes for WEA Message Origination

We observed that sometimes EMA stakeholders simply omitted key quality attributes from the system requirements. Interview data showed that they clearly knew they needed these system qualities. They just neglected to specify them in their RFPs.

As noted earlier, we recommend that EMAs define these quality attributes operationally and include measures. We derived the following list of qualities and definitions from our analysis of stakeholder data. EMAs can use this list to seed thinking about what quality attribute scenarios to create. We do not give specific measures for each of these. As EMAs create scenarios, they should also add measures.

- **Availability:** Ability of a system to mask or repair faults (e.g., service-outage period does not exceed a required value over a specified time interval)

- **Integrability/interoperability:** The degree to which two or more systems can usefully exchange meaningful information via interfaces in a particular context
- **Mobility/accessibility:** Ability to access the alerting software from anywhere
- **Modifiability:** Ability to make modifications to system components without unexpected ripple effects (has to do with minimizing dependency)
- **Performance:** Ability of the system to meet timing requirements
- **Scalability:** Ability to add users or increase system capacity and message throughput as needed
- **Security:** Ability of the system to protect data and information from unauthorized access
- **Testability:** The ease with which the system demonstrates that it meets the user's needs or demonstrates its faults
- **Usability:** Ease with which a user can understand and operate the system

Clearly, an individual EMA's needs vary. While this list reflects the key quality attributes that we gathered from EMAs, organizations should take care to specify the quality attributes relevant to their contexts. We do not include cost in this list because low cost is not a technical requirement; however, cost plays a significant role in tradeoff decisions. Therefore, EMAs will need to consider it as an influential factor as well.

The "quality attribute requirements most likely to be forgotten." After several interviews and RFP reviews, we found that EMAs were more likely to forget to specify some key quality attributes than others. The quality attributes often left out of specification documentation and interview data were security, testability, integrability, and modifiability requirements. In particular, although EMAs identified security requirements as important in many interviews, we did not find security requirements in most RFPs.

With respect to testability, some EMAs expressed dissatisfaction with limited WEA testing options provided by their current alerting and emergency-management product vendors. However, often they had not asked vendors to provide testing alternatives. For example, we talked with several vendors that provide simulation environments and other capabilities about whether their solutions allowed for testing of alert generation (and alerting acknowledgement) without sending a live alert. EMAs could specify such a testing capability in their RFPs.

EMAs often omitted integrability from requirements despite the fact that interviewees indicated they were interested in integrating solutions provided by multiple vendors. These EMAs also desired a seamless interface among the solutions that they used. In this case, a key requirement to consider is the ability to integrate systems and exchange data between them easily (e.g., between a situational-awareness solution and emergency-notification solution). This quality also stimulates other questions, such as "Who will perform the integration between systems provided by multiple vendors? Where will the integrated parts be hosted? How will the 'glue' code be managed and maintained?"

Modifiability was also not often specified as a quality attribute requirement. Many stakeholders were dissatisfied with user interfaces that they could not easily customize or modifications that took a long time for the vendor to complete. This may indicate that the vendor's product rates

"poor" on modifiability. Consequently, small changes become difficult to make or have significant ripple effects.

5.2.5 Examples of Specifying Requirements for Alerting RFPs

We provide some examples in Table 2 of poorly specified and better specified requirements. Whether a particular scenario is well specified depends on the EMA's context.

Table 2: Improving Requirements Specification for Alerting RFPs

Requirement Type	Vague or Incomplete Requirement Example	Improved Requirement Example
Usability	An alert notification message can be sent in a few clicks.	An emergency event occurs, and a user is able to log onto a single system, craft and send an alert within 2 minutes, and do so with a maximum of 3 mouse clicks per operation.
Usability	Speedier message generation with less effort by workforce.	When operators build messages, the graphical user interface (GUI) supports concurrent inputs for multiple message types by simultaneously filling in recurring fields across formats within 2 seconds. Visual cues make clear what new information is required.
Modifiability	The system shall support modification of a templatized message.	The system shall support modification of a templatized message by a trained user within 5 minutes.
Availability	System should be available 24/7.	A fault causes the primary system to crash during peak load, and users experience a maximum of 30 seconds downtime. Overall system availability is 99.9%.
Performance	Ability to send a message to IPAWS-OPEN.	A trained dispatcher is able to construct and send a WEA message under peak system load within 1 minute.
Security	Ability to send a message securely.	An operator is able to send a secure message conforming to xx standards and using xx security products.
Testability	Ability to test the system.	An operator sends a test message, and the system logs the test data and provides simulated acknowledgment of the message within 5 seconds.

Reminder: Requirements depend on a context specific to a particular EMA's needs.

We also observed that the rigor needed for these quality attributes varies; it depends on factors such as an EMA's size, mission criticality, responsibility, and scope of influence. To be clear, we do not advocate a one-size-fits-all requirements approach, and we do not encourage arbitrary reuse of requirements from one RFP into another. This can lead to irrelevant requirements or over-engineering. An EMA can easily spend much more time, money, and effort than necessary if the organization has over-specified its requirements. It is critical to understand what requirements are most important to the organization and focus on specifying those requirements, and only those requirements, to the level that fits the EMA's needs.

5.3 Recommendation

Spend the time to identify the key requirements, and specify them meaningfully.

This is the first step to communicating your needs to potential vendors and to selecting the solution that best meets your needs. Include functional requirements, quality attribute requirements, and non-technical requirements.

Requirements are essential to get right because they drive everything from solution selection, to integration decisions, to implementation, and even definition of test cases. It is important to spend the time thinking through requirements, including current needs, reasonable extrapolations for future needs, and extreme situations that stress the system's capabilities. By properly specifying key functional and non-functional requirements, you can have much more confidence that the systems will meet your demands.

6 Cloud Trends and Considerations for Emergency Alerting

Cloud computing allows people to access computing resources from a remote location, typically over the internet. People use cloud services every day to access email or purchase products. We observed through interviews with EMAs and vendors that many organizations are also moving, or are planning to move, their applications to the cloud. One vendor of emergency alerting systems said that "90% of the RFPs are for hosted offsite solutions."

6.1 Observations

During our stakeholder interviews, we captured the following benefits that EMAs hope to gain by moving to the cloud:

- ability to access systems using mobile devices (from anywhere they can get to the internet)
- improved security
- faster software changes and greater control (modifiability)
- improved availability
- improved scalability and performance
- improved technical support
- lower cost
- elimination of single points of failure

The most important finding in this section is that although EMAs often assume that these benefits will come from the cloud, this is not necessarily true. Whether or not EMAs will receive these benefits depends on how the cloud provider implements the cloud service. Many decisions made by the cloud vendor—such as the software application design, the hardware and network-infrastructure resilience strategy, and level of technical support—determine whether or not the EMA receives these benefits. In this section, we provide an overview of cloud trends we observed, assumptions people make about clouds, and considerations and recommendations for cloud implementations.

Observation 1: EMAs are moving toward public and private cloud-hosted software as a service (SaaS).

In this section, we present the general observation that EMAs are moving to the cloud followed by a brief discussion of the cloud strategies we observed EMAs adopting and why they chose these strategies. First, though, we provide a quick overview of the types of cloud capabilities available. A cloud vendor can provide three main types of capabilities (shown in Figure 11), and these capabilities generally build on each other.

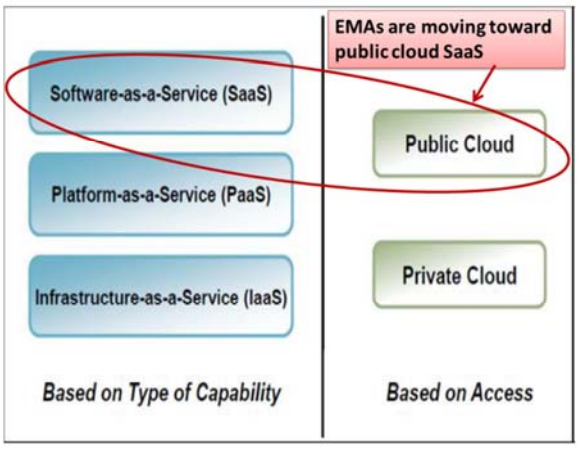


Figure 11: Types of Cloud Services by Type of Capability and Type of Access [Adapted from Lewis 2010]

Starting from the bottom of the figure, vendors can provide infrastructure as a service (IaaS), which includes mainly computational infrastructure (e.g., servers or storage) but does not include a software product. The next level of cloud resource commonly provided by vendors is platform as a service (PaaS). PaaS allows users to leverage vendor-provided resources to create and host applications of a larger scale that they develop themselves. Finally, most of the EMAs we spoke with are moving toward SaaS, in which the vendor provides infrastructure, the platform, and software [Lewis 2010]. With this option, the vendor provides all hardware and software resources at the vendor-managed facility, and the users access the software over the internet.

In addition to the types of cloud resources that vendors can provide, there are also different types of clouds (also shown in Figure 11). The two most common cloud options are public and private clouds. Public cloud resources are accessible over the public internet and are typically provided by a commercial vendor. Private cloud software is hosted by an enterprise for the users within the enterprise boundaries (for example, the EMA enterprise). Only users within the enterprise network boundaries can access the private cloud resources. We observed both of these cloud options in use by EMAs. The majority of the small to mid-sized EMAs we spoke with were moving to a public-cloud SaaS option (circled in red in Figure 11) because they had limited resources and sought to avoid the cost of hosting and managing applications.

We also observed that some of the larger EMAs, generally county- and state-level organizations, were creating their own private clouds. In this approach, the larger organization hosts the private cloud and provides the service for jurisdictions under its purview that do not have the budget for their own emergency-management solutions. The organization hosting the private cloud manages support for the solutions and controls user access.

Observation 2: EMAs make assumptions about the quality of service (QoS) provided by cloud vendor products without understanding the key tradeoffs of the vendor's technical strategy.

We observed that EMAs often assumed the existence of consistent standards for QoS across the vendor cloud community for emergency management. We heard EMAs use terms such as "standard enterprise quality of service (QoS)" when describing the QoS that they expected from their

new cloud-based solution. The problem is that standard enterprise QoS does not exist. There are no standards for QoS across commercial off-the-shelf (COTS) products. Attributes, such as level of resiliency, vary depending on design choices and implementation decisions. In the rest of this section, we discuss some examples of technical decisions related to cloud environments that can have significant implications for QoS.

6.1.1 Shared Resource Considerations

Some EMAs said that the ability to add users (scalability) and get alerts to citizens rapidly (performance) were important qualities that they expected from their cloud-based applications. However, performance of software hosted in a shared cloud environment depends on the shared-resource technical strategy. For example, an alert-generation service provider may host several instances of the alerting software for different jurisdictions on the same equipment.

We suggest that it may help EMAs to become familiar with some of the shared-resource options and their tradeoffs. Figure 12 shows multiple tenants sharing cloud configurations in three examples from SEI's cloud computing tutorial [Lewis 2011].

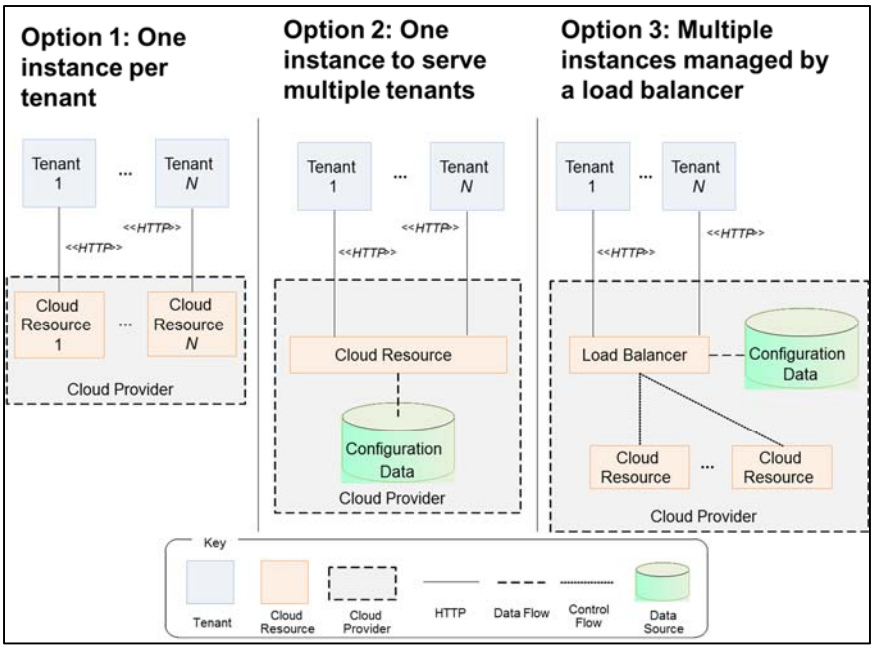


Figure 12: Configurations for Sharing Cloud Resources [Reprinted from Lewis 2011]

The example shown in Option 1 assigns one instance of cloud resources (infrastructure and software) per tenant. This option provides the most consistent and reliable performance because there is no potential impact by other tenants using common resources; however, this option is typically more expensive than Options 2 and 3. Option 2 illustrates a single set of resources shared among tenants. Some vendors allow a tenant to pay to get more resources than other tenants. Option 3 illustrates multiple resources managed by a load balancer so that resources can be dynamically allocated to tenants as needed. This option is more complex for the vendor to manage but allows for maximum use of resources. Depending on the sharing arrangement and design configuration, the EMA may get varying qualities of service.

6.1.2 Cloud Resiliency Considerations

Managing resiliency is about protecting people, processes, technology, and data against loss during an incident or disaster [Caralli 2010]. In this section, we focus on the technology and data-related resiliency considerations for cloud-based applications. There are two major resiliency considerations when EMAs move to a cloud-based application strategy. First, internet connectivity is critical so that users can access cloud resources particularly during an emergency situation. We talked with EMAs that had as many as three tiers of internet redundancy, including cable-based internet access, satellite, and wireless modem.

Second is the resiliency of the cloud-based solution itself. In our interviews, we observed that many EMAs assume that their new cloud-based solutions will be more robust than their existing solutions (e.g., be less prone to outage, able to recover more quickly if an outage occurs, and configured with redundant data storage). The reality is that resiliency strategies and tactics provide different levels of service. Figure 13 provides a simplified illustration of some of the redundancy strategies offered by the product vendors and EMAs that we interviewed.

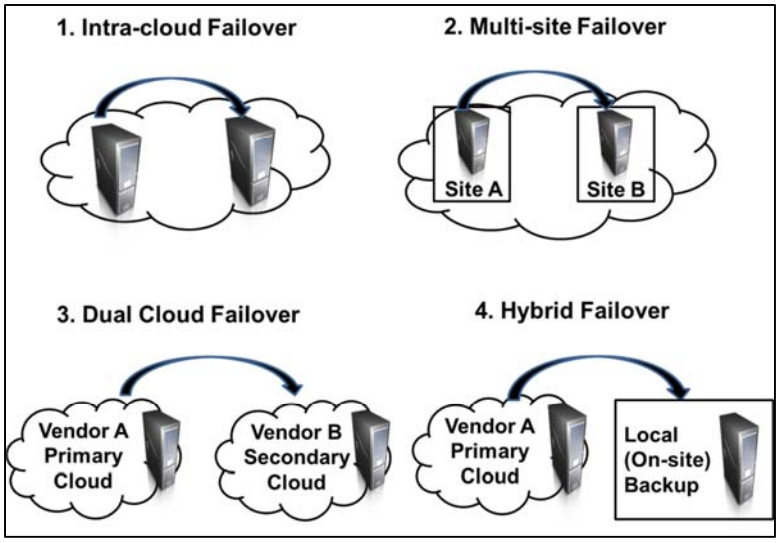


Figure 13: Redundancy Strategies for the Cloud

1. **The intra-cloud failover strategy** provides software and storage redundancy within the same geographic location in a vendor cloud. This is the least expensive option of the four shown here; however, it is also the least resilient option since a large-scale disaster could potentially take out the primary and secondary servers.
2. **The multisite failover strategy** is similar to Option 1 but adds the dimension of failing over to a separate geographic site. The geographic separation of the primary and secondary sites provides additional protection. However, since the same vendor owns both the primary and secondary sites, there is still some risk that if the vendor went out of business or was attacked both sites could go out of commission. This is a common cloud-resiliency strategy and is appropriate for organizations that need a moderate to high level of resiliency.
3. **The dual cloud strategy** provides primary and secondary cloud-based sites with failover to a second cloud site typically at another geographic location. The secondary site is owned and managed by a different vendor. In this case, the user is either automatically or manually redirected to another website if the first one goes down. This is an expensive option because it

requires contractual arrangements with two different vendors. In addition, if capabilities such as situational-awareness or incident-management solutions are bundled with the alerting capability, it may be challenging to synchronize data across disparate systems. This option would be appropriate for organizations requiring very high levels of resiliency such as state-level or very large county EMAs.

4. **The hybrid failover strategy** has a cloud SaaS application as the primary site, which fails over to a locally hosted site for backup (alternatively, the local site is the primary site and fails over to the cloud backup). This strategy offers the most resilience because there is no interdependency between the primary and the secondary providers and the local site provides a great deal of control. However, this option is expensive and complex. As with the dual cloud strategy, if capabilities such as situational-awareness or incident-management solutions are bundled with the alerting capability, it may be challenging to synchronize data across disparate systems.

These are not the only possible cloud-based integration options. Vendors could offer an essentially unlimited number of configurations. In addition to these four high-level resiliency strategies, vendors also use a variety of more granular tactics within the cloud environment to provide additional degrees of resiliency. For example, some vendors provide active failover. When an active-failover tactic is applied, primary and secondary servers run concurrently so that if a primary server fails the secondary server continues to service requests with no downtime. Another alternative, which is usually less expensive than active failover, is passive failover, in which the vendor can quickly put a backup node in place if the primary fails (sometimes with manual intervention) with minimal downtime.

6.1.3 Security Considerations for Cloud-Based Applications

Many EMAs also assume that they will have a more robust security architecture when they move to a new cloud-based solution. However, this depends on the vendor implementation. Vendor choices for security architecture do not always match EMAs' needs. The mechanics of implementing a secure solution falls primarily on the cloud vendor, but the risk of security failure primarily impacts the EMA. Cloud vendors must protect messages and data being exchanged over the internet, hardware infrastructure, software applications, and even user-authentication information. Vendors should exhibit strong security practices at all times, but we observed that this does not always happen. For example, we attended a demonstration of a vendor emergency-warning product where the demonstrator logged into a production website using a *real EMA staff username and password*. This raises concerns about how seriously the vendor is taking security.

EMAs should also keep in mind security considerations even when using a cloud-based solution. For example, certificates are required to authenticate a user on the cloud-based SaaS solution. It is important to store the certificates securely and protect them. We suggest that EMAs should know their own security requirements and ask the vendors how they will meet those requirements in a cloud-based system.

EMAs desiring to move toward cloud services need not become cloud computing experts. Rather, by understanding some of the areas where cloud technical strategy can have a big impact on QoS, EMAs can be better prepared to probe vendors to ensure that they will get what they expect from their cloud solutions.

6.2 Recommendation

Know what QoS you need, and ask how the vendor will achieve it.

We hope that we have emphasized the idea that there is no standard enterprise resiliency or QoS when it comes to cloud-based solutions. The QoS characteristics of a cloud-based solution depend on the technical strategy employed by the cloud provider. We have two recommendations: (1) clearly and concisely specify your QoS needs, and (2) ask how the vendor will achieve them. Section 5 of this report discusses a scenario-based approach for specifying QoS requirements. If you begin with measurable, well-specified requirements, you can use them later to evaluate vendor cloud technical strategies and determine if they will meet your needs. After you have specified the QoS requirements, use them to compare cloud-based solutions. See Table 3 for a set of questions you can ask vendors to understand the risks and tradeoffs better.

Table 3: Questions to Ask the Cloud Vendor

Drivers	Questions to Ask Cloud Vendor
Improved accessibility and mobility	How does the cloud implementation support accessibility and mobility?
Minimized security vulnerability	What are the security-architecture strengths and weaknesses?
Fast software changes, greater control (modifiability)	Is customization allowed, and how rapidly can you make changes? When are updates scheduled?
Improved availability	What level of availability does the cloud architecture provide?
Improved scalability and performance	What level of scalability and performance does the cloud architecture provide?
Improved technical support	How responsive is technical support?
Elimination of a single point of failure	What failure scenarios have you examined, and how will you deal with them? Have you considered weaknesses such as single point of failure?

7 Considerations for Protection Against Cybersecurity Risks

The information in this section is a brief summary of the comprehensive *WEA Service Cybersecurity Risk Management Strategy for Alert Originators* [SEI 2013]. That report describes the CSRM strategy in detail and provides example results from executing the strategy.

The AO community encompasses organizations of varying jurisdictional size that may have few or many resources available for technology adoption, including resources to be applied to cybersecurity. Across the many organizations that we interviewed, we discovered a general lack of awareness of AO vulnerabilities that may enable cyber attackers to modify, delay, destroy, or spoof WEA messages. We therefore recommend that AOs establish an awareness of the risks of cyber attack throughout their organizations and apply a cybersecurity risk management strategy focused on preventing, detecting, responding to, and recovering from cyber attacks.

7.1 Observation

Observation: Most organizations do not possess a concrete and comprehensive awareness of the cybersecurity risks that they face daily.

Based on interviews conducted with a number of AOs, we conclude that cybersecurity risks are not well understood by most EMAs. Without such awareness, it is difficult to develop a culture of security and clearly articulate essential roles and responsibilities for mitigating the risk of disruptive cybersecurity incidents. When asked about security practices, many AOs mentioned the use of passwords but did not identify rules for access control, training, or other information that would indicate sufficient awareness of risks and protective mechanisms. Some AOs admitted that for simplicity, individuals working the same shift shared user accounts or that all user accounts were assigned administrative privileges, both high-risk practices. Finally, we discovered that some AOs have posted information on the public internet that may facilitate both technical and social-engineering attacks on alerting systems.

7.2 Recommendations

We recommend that AOs take the following actions to reduce susceptibility to cyber attacks.

Learn about the security risks associated with modern alerting technologies, and establish a culture of good security.

EMAs should learn about the risks associated with technologies that they have recently adopted or plan to adopt and how seemingly simple acts can greatly increase vulnerability. For example, enabling connectivity to the internet from previously isolated devices, using mobile devices to access organizational resources, and allowing removable media on critical systems can all make the EMA vulnerable to cyber attack. Education is only the first step. EMAs should then establish a culture of security, with policies, procedures, and training to instill basic risk awareness and good security practices throughout the organization.

Implement a cybersecurity risk management strategy.

EMAs should also implement the four-part strategy described in Sections 3–6 of the *WEA Service Cybersecurity Risk Management Strategy for Alert Originators* [SEI 2013]:

Part 1. Prepare for cybersecurity analysis by documenting the environment and operational sequence of steps involved in alert generation.

Part 2. Identify threats and vulnerabilities that may interfere with the alert-origination process by analyzing the operational sequence of steps documented in Part 1.

Part 3. Assess and prioritize risks associated with the threats and vulnerabilities identified in Part 2.

Part 4. Define cybersecurity risk-mitigation roles and responsibilities, and mitigate risks identified in Part 3.

Figure 14 illustrates the four-part CSRM strategy. The figure highlights the necessity to revisit applicable parts of the strategy to address changes in operational procedures, alerting technologies, techniques used by attackers, the organization's risk tolerance, and organizational roles and responsibilities.

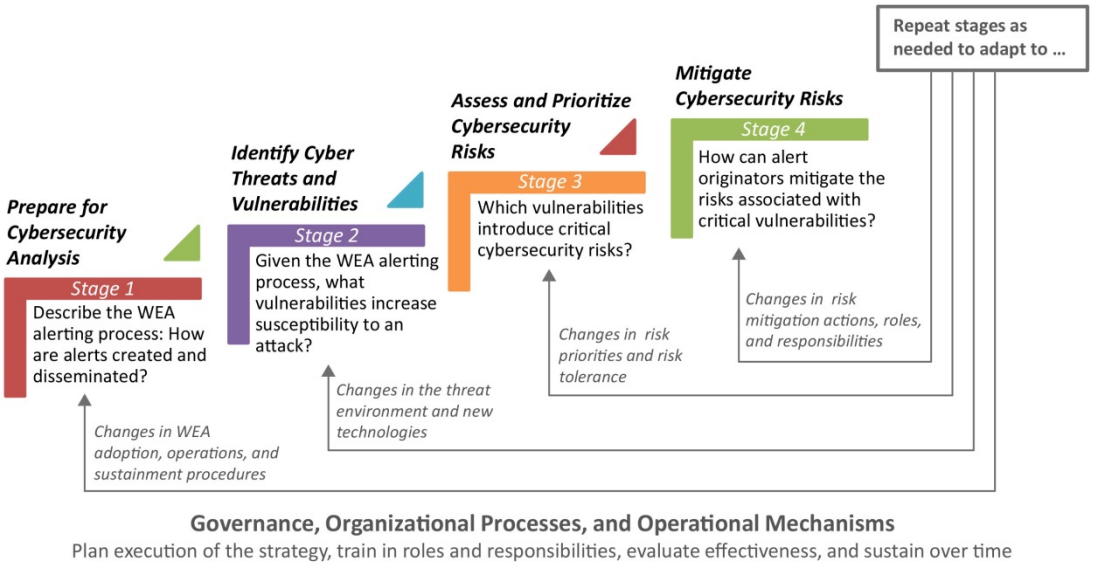


Figure 14: Four-Part Cybersecurity Risk Management Strategy for WEA Message Originators

To govern implementation of the CSRM strategy, we also recommend that AOs develop a plan that defines cybersecurity policies and procedures related to adopting WEA and cybersecurity risk-mitigation roles and responsibilities. EMAs should also plan an approach to executing the four-part CSRM strategy.

8 Considerations for WEA Product Selection

Most EMAs will buy an emergency alerting product from a vendor, as opposed to developing a solution in-house. The goal when purchasing a vendor solution is that it will meet the organization's expectations. The considerations for integration, hosting, requirements, and security that we discussed in previous sections now form the foundation for making the appropriate decision to support the desired outcomes.

8.1 Observations

This section comprises three observations:

1. Product selection is becoming more complex.
2. EMAs may select product features without sufficient consideration of organizational expectations.
3. There is a tendency to overlook possible consequences of tradeoffs across features and quality attributes, rather than analyzing and factoring them into selection decisions up front.

Observation 1: Product selection is becoming more complex.

In Section 4: Integration Strategy Considerations, we shared the observation that the EMA integration environment is becoming increasingly complex. Despite long-term experience with emergency-alerting products, EMAs acknowledge the growing technical challenge of determining what capabilities they need now as well as what they may need in the future. EMAs are also challenged by the number of products and features available to them. While strong domain knowledge in emergency operations certainly helps, it does not always provide EMAs with the technical expertise to develop thorough and accurate requirements specifications for vendor products (discussed in Section 5: Requirements Considerations). While EMAs increasingly depend on software solutions for critical capabilities during an emergency, we noted a greater focus on people and processes than technology-related topics at the emergency-management conferences we attended.

Observation 2: EMAs may select product features without sufficient consideration of organizational expectations.

Regardless of the type of solution, every selection process requires balancing a number of equally important criteria. The task becomes more difficult when those criteria conflict with each other. In one case, an EMA chose a free product that would be quick to deploy. The EMA wanted to incorporate a WEA message-origination solution as easily as possible and expected to replace it in a relatively short time with more robust capabilities. Because of the expected limited use, they did not plan for integration of the free product with their other emergency software in their selection or deployment plans. What they discovered was that even a free solution has hidden costs. Operators had a hard time remembering how to use the product from one time to the next because of poor screen design. And without integration, a high-profile alert required the additional time and stress of creating the message in multiple formats.

Another common expectation among EMAs is the belief that vendors can quickly implement software changes. Some organizations we interviewed were frustrated by lengthy delays for re-

quested changes. However, the speed of new releases is unlikely to change unless the EMA negotiates this in the requirements or contract with the vendor. To make matters worse, feature upgrades or unscheduled changes may negatively affect the EMA.

Observation 3: There is a tendency to overlook possible consequences of tradeoffs across features and quality attributes, rather than analyzing and factoring them into selection decisions up front.

Product and feature decisions are actually design decisions in disguise. For example, decisions to improve the speed of performance can negatively influence complexity or modifiability [Bass 2012]. Table 4 shows some of the common EMA quality attribute desires (left column) and the typical tradeoffs, that is, qualities that may be negatively affected (right column) by an emphasis on the desired quality [Bass 2012].

Table 4: Potential Product-Quality Tradeoffs

Promoted Qualities	Possible Negative Impacts
Availability	Maintainability, Complexity
Security	Performance
Front-end integrability (seamless interface with a "one-product" feel)	Vendor lock-in
Back-end integrability	Performance (runtime), Complexity
Modifiability	Performance, Security
Performance (typically speed of response)	Complexity, Modifiability
Scalability	Complexity
Usability	Complexity

Before EMAs choose a WEA solution, they should recognize that some desirable qualities in a software product or service can negatively impact other desirable qualities:

- Promoting availability typically involves applying fault-tolerance and/or redundancy tactics. This may involve adding additional hardware and software components, increased complexity, and more difficulties in maintenance.
- Promoting security can affect performance due to the overhead from additional architectural layers needed to protect data and other resources as well as to guard against and recover from attack.
- Similarly to security, promoting modifiability (i.e., software can be easily modified) can affect performance. A common design tactic that enables modifiability is to add layers to the architecture in order to encapsulate components and localize the impact of changes. These additional layers can result in slower system responsiveness. In addition, more layers can negatively affect security because they can introduce additional vulnerabilities at points where the system components interface with each other. For example, if an EMA wants to be able to change message-template functionality without affecting the rest of the system, it might implement the message-template module as a separate module encapsulated by an interface. If this interface is made accessible so that it can be leveraged by multiple products (in other words, so the EMA can use the same message-template capability from its alerting product, situational-awareness product, etc.), then this interface could likewise be used by attackers to damage and degrade the message-template capability.
- Promoting front-end integrability (a seamless interface) in this domain usually means purchasing a single product that "does it all." This can introduce vendor lock-in. *Vendor lock-in* is a business risk that limits a customer to working with a single vendor and the products it

produces. Switching to another product or set of products then becomes a costly decision because this typically means a wholesale replacement of all components.

Cost is not a system quality but is a prominent decision factor in product selection among EMAs. A low-cost product can have architectural limitations that may not emphasize qualities such as modifiability, usability, and so forth.

8.2 Recommendations

Confirm WEA capabilities before purchasing the product.

- Ensure that the advertised solution does offer WEA capability by reviewing various vendor sites for keywords and phrases such as CMAS, CMAS/WEA, or WEA; Common Alerting Protocol (CAP 1.2); IPAWS-OPEN; eXtensible Markup Language (XML) and/or Emergency Data Exchange Language (EDXL); "no opt-in alerting"; and "transmission to public via cell tower broadcast."
- Require a pre-purchase live demonstration of the WEA product at the EMA to confirm existing capability and operational soundness of the product. We also found that many vendors can demonstrate products from remote locations by leveraging webinar or other live-meeting capabilities. It would also be useful to ask the vendor to supply references from other customers who use the product.
- Request confirmation from the vendor that the product has passed Supporting Technology Evaluation Project (STEP) Testing. The FEMA National Preparedness Directorate offers this project to assist the response community with interoperability test and evaluation and as a means for determining product compliance with CAP 1.2 and IPAWS-OPEN. Commercial software-system developers may voluntarily submit their products to the Preparedness-Technology, Analysis, and Coordination (P-TAC) Center's STEP for independent testing of conformance to the CAP, EDXL, and IPAWS specifications [FEMA 2013e]. Evaluation reports are published on the Responder Knowledge Base website (www.rkb.us).
- Seek opportunities to obtain additional expertise in software selection as part of conference workshops, EMA mentoring programs, and academic emergency-management curricula.
- Consult with other jurisdictions that are similarly sized and have similar profiles, and circulate lessons learned and best practices in developing specifications.

Develop a customized prioritization method that documents the progression from operational expectations to prioritized features.

- Define and prioritize a list of desired organizational expectations or outcomes.
- Determine the capabilities that the WEA product must have to support the expectations, and pair them with the prioritized expectations.
- Link the WEA capabilities to specific features. We recommend that emergency managers and other personnel get involved in product selection. The approach will allow backward traceability from operational objectives to ultimate feature prioritization.

EMAs that lead tradeoff discussions should acquire sufficient knowledge of tradeoff definitions and consequences to lead these design discussions.

- Be specific about how the qualities you want might affect other qualities of the product or service. An organization's unique operating context determines the positive or negative im-

pact of a specific tradeoff decision. The common tradeoffs shown in Table 4 are not the only tradeoffs, and tradeoff analysis requires technical background and experience in the domain. It is also important to recognize that requirement specifications can drive faulty tradeoff decisions.

Fill the role of a "lead integrator" if you will use multiple vendor products.

- Don't underestimate the difficulty of this task. Either hire a vendor to perform this role or assign someone within the EMA to perform this role if there is sufficient expertise.

9 Testing Considerations

Many EMAs will purchase COTS products for WEA messaging. While these products have been subjected to some amount of testing, the vendor cannot test in the context of the EMA's specific environment. EMAs should take responsibility for testing the alerting system in their own contexts. The term *context* refers to any element external to the COTS product that might affect its operation, including the hardware, operating system, networking hardware and software, and other software that will be operational during an emergency.

9.1 Observations

An overview of key testing-related observations follows:

- There is a lack of understanding about what environments are available for EMAs to test their ability to send alerts using the WEA service.
- EMAs are uncertain about the types of software and system tests that they should conduct.

Observation 1: There is a lack of understanding about what IPAWS environments are available for testing the WEA service.

EMAs were often unsure about what testing options are available for testing WEA messaging. Several testing options for WEA do exist. Figure 15 summarizes options for testing CAP-compliant systems available to EMAs, vendors, and carriers [FEMA 2013b].

Figure 15: Three IPAWS Testing Environments [Adapted from FEMA 2013b]

Testing Option 1: PROD. PROD stands for "Production" and represents the production system through which real alerts are sent to the public. PROD, or live, testing requires FCC and federal consent. The live testing approach was used for a New York City demonstration on December 15, 2011. While PROD enables the sender to test the production system integration from end to end, sending live alerts for testing is prohibited. The current rules reflect wireless carrier industry concerns (e.g., over-alerting, subscriber cancelations) rather than the potential for misinterpretation of the test alert by the public [CFR 2012b]. While for completeness we include this option, it is not an option for most EMAs. An EMA must submit a waiver request to the FCC to send production alerts.

Testing Option 2: Test Development Lab (TDL). TDL is a test environment that maintains a working instance of the next version of IPAWS-OPEN to be deployed. This environment is primarily for alert-origination vendors to test their equipment and software with the new version of IPAWS-OPEN before it is deployed to the PROD system.

Testing Option 3: Joint Interoperability Test Command (JITC) Test Laboratory. In the JITC test lab, EMAs, with the help of their vendors, can connect to an IPAWS-OPEN test environment and test their WEA software. The JITC lab is completely separate from the production IPAWS-OPEN environment, so alerts are never disseminated to the public. The JITC lab has a simulation environment that mimics the capability of the EAS and WEA infrastructure for testing (although the hardware is not the same). EAS alerts are routed to EAS/CAP devices in the lab, and WEA messages are routed to a simulated CMSP Gateway to a "toy cell" (a low-power cell tower in the lab). Note that the alerts coming out of the IPAWS-OPEN environment are routed to a CMSP Gateway; however, they do not traverse any CMSP infrastructure. WEA-capable handsets in the lab receive and display the WEA messages. The accuracy of these simulations is not known at this time.

FEMA is conducting aggressive outreach to inform EMAs of these testing options and resources. FEMA encourages any EMA to use the resources and vendors to make the JITC test environment available to their clients [JITC 2011]. The JITC lab is in Indian Head, Maryland, and visitors are welcome. If simulated end-to-end testing is a critical need for your organization, we suggest asking candidate vendors if they have a testing capability integrated with JITC. If your vendor is not coordinating with the FEMA IPAWS-OPEN team, request that they do so. Your organization can also collaborate with other EMAs to participate in test activities. Again, be aware that part of the alerting pipeline, from IPAWS-OPEN onward, is simulated rather than executed on a production system.

Observation 2: EMAs are uncertain about the types of software and system tests that they should conduct.

Most of the EMAs we interviewed realized that they should do some alert-generation testing. However, they typically limited the scope of this testing to creating and sending an alert message to IPAWS-OPEN. The test cases employ scenarios that assume that all the right conditions exist for successful alert origination and nothing goes wrong along the way (e.g., no interface mismatches occur with FEMA IPAWS-OPEN, security certificates are valid, and connections to IPAWS-OPEN and to CSMPs are working). There are drawbacks to this approach. First, these types of tests often do not focus on the problem spots where critical failures arise. Second, this approach limits the testing scope to the activities that occur before and during message generation. As discussed in Section 4: Integration Strategy Considerations, some of the failure points may occur after the message goes out, and EMAs need to analyze and test these points as well. To develop tests that cover these cases, it is necessary to think about how failures can occur through the system one component at a time and reason about component-failure scenarios at key points such as the IPAWS interface, alerting software, and cross-organizational boundaries. We discuss strategies to address these considerations in the Recommendations section.

9.2 Recommendations

Based on our observations and the discussion in this section, we make the following recommendations for EMAs:

- Attend FEMA IPAWS webinars and outreach sessions to stay current with and take advantage of evolving testing platforms and tools.
- Develop test cases based on the different components involved, and conduct periodic tests of the individual systems and software, including interface testing between the alerting software and IPAWS-OPEN, using available testing platforms. Leverage a conceptual testing framework as described in the following WEA-specific example.

Example Conceptual Reasoning Framework for Testing WEA-Capable Solutions

We derived this example of a conceptual framework for testing WEA-capable solutions from our interviews and collected data. Because a WEA system is made up of many components owned by a variety of organizations, we describe the framework as a progressively growing chain of system components. Figure 16 shows three different chains, beginning at the bottom with the locally installed software product in isolation and gradually extending toward the public. With each new link in the chain, a local EMA will encounter additional restrictions on what a test can accomplish. As much as possible, the EMA should coordinate with the vendor of the system or the state EMA to leverage testing activities of these two organizations. We discuss each of these chains in terms of the types of tests that EMAs should run and the types of defects that the test can help identify. We begin the discussion with the isolated local system.

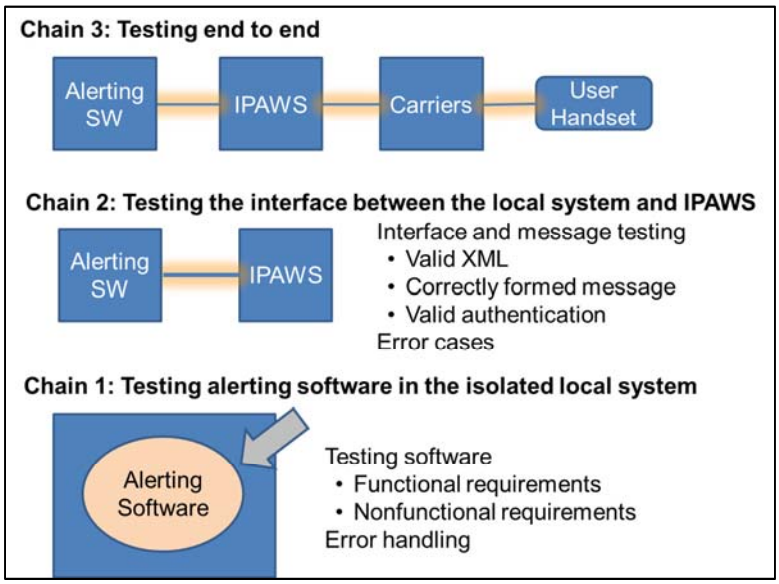


Figure 16: Three Types of Testing Applicable to WEA

9.2.1 Testing Alerting Software in the Isolated Local System

The local alerting system includes solutions for authoring and sending alert messages. That system may reside on hardware that also hosts emergency-management systems and other supporting software. Although the vendor has tested the product, the customer still has responsibility to test items that the vendor cannot test, namely, how the system will interact with other software used in

a particular EMA installation. We observed situations where the EMA thought the vendor covered system-related testing and the vendor thought the EMA covered testing, so there was a risk of not sufficiently testing the WEA capability.

An EMA should test its vendor-supplied system to determine whether it meets the system requirements. These tests, often referred to as *user acceptance tests*, determine that the system can do what it is supposed to do (functional requirements) within the given constraints (non-functional requirements). Figure 17 illustrates. To select the test cases for this testing, first consider the functional requirements of the system and then consider the non-functional (quality attribute) requirements (see Section 5 for definitions).

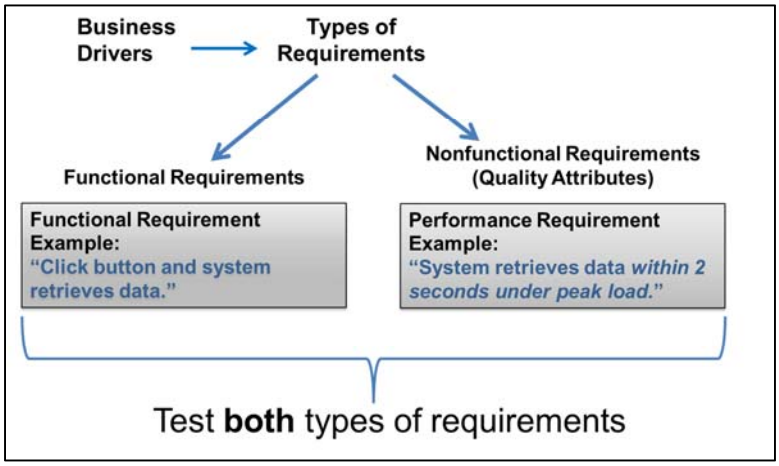


Figure 17: Testing Against Requirements

Functional testing. Functional testing involves testing the functional requirements defined in the requirements specifications. Basic functional test cases should include, of course, the ability to create and send a WEA message. Emergency-management standard operating procedures are a very good source for functional test-case ideas. An EMA should also test any additional functional aspects that the alerting system supports, such as message-template creation and modification as well as the ability to define and change alerting roles, privileges, and rules.

Since the vendor will have tested most of the standard functions, an EMA should test exceptional scenarios (e.g., an operator hits "cancel" right after sending an alert). It is also important to test whether the system gracefully handles failure conditions, including network failures and local disc errors.

Non-functional (quality attribute) testing. In addition to testing functionality, an EMA will need test cases for testing requirements related to quality attributes. What the EMA needs to test will depend on the hosting strategy (e.g., locally hosted and managed by the EMA, or hosted and managed by the vendor). Some examples of tests related to WEA quality attributes are performance, usability, resiliency, and security testing.

- *Performance testing.* To test how rapidly the system responds, EMAs could develop a test case to send multiple system requests (e.g., alerts) concurrently and monitor for system responsiveness to determine if performance degrades beyond an acceptable limit. Since it is unlikely that EMAs will need to send multiple WEA messages concurrently (with the exception of a national-level organization such as NWS), EMAs could develop performance test cases

to investigate the resiliency of system resources on which the system depends. For example, EMAs could test and monitor for network latency while under heavy load, such when a network is shared between multiple distributed systems while in use.

- *Usability testing.* Usability tests typically involve observing the operators as they use the features of the system to perform a task. For example, a test case may involve monitoring operators as they send a WEA message while capturing the time it takes to log on, create, and send a WEA message. This data is particularly important if the operators must use multiple systems during an emergency situation.
- *Resiliency/availability testing.* For locally hosted systems, EMAs should test hardware, network, and software components on a regular basis. For example, if power sources, local networks, internet connectivity, servers, and software are replicated, tests should verify that software and hardware components failover properly if the primary component fails (e.g., the server on which alert-origination software is running). If separate backup systems are used, EMAs should test them each time they test the primary system. If using a cloud SaaS, we suggest requesting that the vendor provide evidence of regular testing for all software and system components and that results are within acceptable limits.
- *Security testing.* The STRIDE model can be used to develop vulnerability test cases. See Section 4 of the *WEA Service Cybersecurity Risk Management Strategy for Alert Originators* for more detail [SEI 2013]. STRIDE includes six categories of threats (its name is formed from the first letters of the category names): spoofing, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege.

EMAs should run these tests when the system is initially installed and should repeat them periodically. Automated test tools reduce the effort required to apply tests to the system. Automating tests usually involves writing test procedures in a scripting language that is much easier to use than a full-strength programming language.

Tests should be repeated periodically or at a minimum every time there is a change to the system (e.g., new hardware installed, drivers updated). If the tests are automated, running all the tests available should take very little time. If the tests are not automated, EMAs or vendors can create a regression-test suite by selecting the tests that exercise the most important system characteristics. The purpose of these tests is to verify that functions that were working have not regressed to a non-working status. If a COTS vendor is providing the alerting capability, a good question to ask is whether the vendor conducts regression tests, particularly after making changes to the system.

9.2.2 Testing the Interface of the Local System to IPAWS

In this section, we discuss a first level of system-integration testing that focuses on the interface between the alert-origination system and IPAWS-OPEN. This level of testing stops short of dissemination to carriers. EMAs should apply interface tests periodically to test the interface from the EMA's WEA solution to IPAWS-OPEN. The New York City demonstration, which involved sending a message and manually verifying that it was received by people using handsets in that jurisdiction (not automated testing), is one example of WEA testing [Trocki Stark 2013]. Interface testing can help ensure that interfaces work properly and that nothing has changed that could cause an alert request to fail. If you use a vendor product that is IPAWS-OPEN compliant, the vendor may run system-integration tests and should provide test reports. The vendor may also provide a simulator that supports running test cases outside the live PROD. Interface testing can

validate syntactic (proper structure) and semantic (proper meaning) interoperability for messages, including

- adherence to the CAP standard and the IPAWS-OPEN CAP Profile
- adherence to the 90-character message limit
- correctness of the values sent in the <certainty>, <severity>, and <urgency> fields
- validation of any rules (e.g., alert message cannot specify an <area> value for a region for which the AO is not authorized to issue an alert)

9.2.3 Testing End to End

Here we focus on testing the system from end to end, to include the sending of alert messages, the receipt of the messages, and the usage of technology by the public to respond and react to the messages (e.g., websites, social media, phones, call centers). These end-to-end testing scenarios introduce a variety of new concerns beyond system-integration concerns. For example, handset platforms can vary widely in terms of displays and features, so end-to-end testing must take multiple platforms into account.

Testing at this scale requires tactics beyond those used for single systems or even distributed systems. Analysis approaches should allow for cross-system and cross-organizational scenarios. Several EMAs we spoke with participate in large-scale, multi-organizational exercises such as simulated hazardous spills or severe-weather response scenarios, so the emergency-management community has a strong foothold in this area. For example, the State of Texas has exemplary exercise practices [Texas DPS 2013].

We suggest that mission thread analysis (described in detail in Appendix C) may be useful in identifying productive test cases. Mission threads describe a cross-organization business process, such as responding to an emergency. An analogous example of how mission thread testing has been used at this scale is derived from the Department of Defense (DoD) cybersecurity community. For cyber-attack exercises, the DoD needs to coordinate across several organizations (much like responding to a national emergency event). The DoD has used mission threads to develop, analyze, and validate end-to-end, cross-organizational scenarios. The mission thread approach helped identify possible points of failure (e.g., performance bottlenecks) and determine needs for automated capture of information during the test (e.g., effectiveness of systems or people, system failures, and system-response rates).

As illustrated in Figure 18, EMAs can develop the mission thread steps that have testing considerations into test cases. The tests may require the collaboration of multiple agencies. We illustrate mission thread testing through a hypothetical, generalized Hazardous Materials Mission Thread.

- Mission Thread Step 1: A chemical spill occurs, and a WEA message is sent.
- Mission Thread Step 2: First responders arrive and begin to manage the hazard.
- Mission Thread Step 3: Citizens receive a WEA message. The 911 call center or Public Safety Answering Point (PSAP) starts receiving calls but is quickly overwhelmed with the volume of calls.

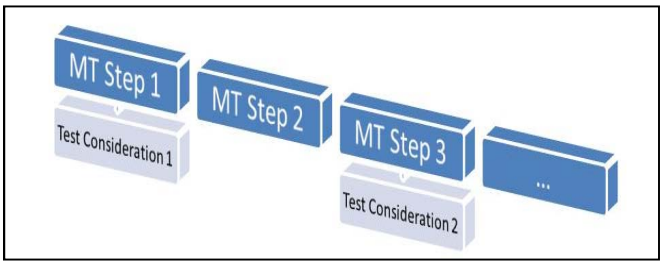


Figure 18: Mission Thread Testing Approach

Mission thread analysis is useful for developing end-to-end WEA testing cases because it helps focus analysis efforts on areas where failure points can have great impact. For example, we use mission thread analysis to identify critical places in an emergency scenario where technology must support, and scale, during a crisis and failure could affect safety or cause loss of life. We illustrate this concept in Figure 18. Step 1 spawns the test case for Test Consideration 1. An EMA could develop a test for sending a WEA message based on this type of emergency. This may include more detailed scenarios such as the ability to send an alert if the spill affects the EMA's critical infrastructure or there is a heavy use on network. Step 2 does not leverage technology or systems; therefore, we do not show a testing consideration in that step. Step 3 could spawn a test case for Test Consideration 2, testing of maximum calling capacity. This is particularly important if the limitation is due to constraints beyond the number of available phone lines or people. If instead the limitations in capacity are due to supporting call-center software or systems, this would also be an important area to test and a potential target for improvement.

10 Operational Considerations

WEA adoption obviously will affect EMA operations. EMAs will not use WEA as a stand-alone service but will weave it into the overall emergency-management operations. A complete exposition on EMA operations is beyond the scope of this document. However, we gleaned some operationally relevant information by working with several early adopters of WEA. Information in this section reflects the results of Mission Thread Workshops, as well as site visits with other EMAs, interviews, conferences, analyses of RFPs, and other stakeholder interactions.

10.1 Observations

This section contains the key observations on operational considerations:

- Many organizations lack a method for identifying the operational impacts of WEA adoption.
- EMAs recognize the need to address and manage operational challenges prior to an emergency incident.
- There are existing practices that can assist EMAs in sending rapid, clear, and timely messages during an emergency.
- Large-scale exercises and training are important to exercise cross-agency and cross-system scenarios.
- There are cross-organizational and media-channel coordination challenges in issuing WEA messages. These challenges existed before WEA was introduced; however, WEA adds another alerting capability to the mix.

Observation 1: Many organizations lack a method for identifying the operational impacts of WEA adoption.

The organizations that we spoke with all had existing emergency-management and warning systems and, consequently, they also had existing operational procedures. The question that several stakeholders seemed to be struggling with was “How will WEA impact my existing operational procedures?” EMAs often lacked an effective way to identify these impacts.

To gather data for our report and concurrently help these organizations with this challenge, we conducted two Mission Thread Workshops (MTWs). The MTW is a facilitated analysis approach useful for large-scale, cross-agency systems analysis (see Appendices C and D for details). Typical output of the MTW is identification of procedural and technical risks. This approach proved useful during the analysis phase of this report for identifying common themes and challenges faced by EMAs.

We summarize the general approach to MTWs here. Stakeholders from multiple organizations that are involved in emergency alerting and warning across a jurisdiction are invited to attend the workshop (the broader the set of stakeholders, the better). The MTW session uses custom-developed mission threads created before the session. The facilitator walks the stakeholders through the steps of the mission thread as a group. The key output from the mission thread process is a set of risks or challenges that may warrant further attention. To illustrate this, Figure 19 contains a mission thread snippet pointing out where participants have identified a challenge.

Step	Description	Engineering Considerations, Issues & Challenges
1	A large truck carrying pesticides goes through an intersection with a "RED" traffic light and is hit broadside by an SUV. Both vehicles burst into flames.	N/A
2	Several witnesses in cars that were approaching the intersection stop and call 911 to report the accident. Others rush to assist the accident victims.	• 911 call center/PSAP starts receiving calls but is quickly overwhelmed with the volume of calls. • The 911 calls roll over to neighboring 911 call centers/PSAPs.
3	The driver from the SUV is pulled from the vehicle and placed on a nearby lawn.	• Fire, police, and EMTs are dispatched to the scene. • …
4	Fire rescue and police arrive on the scene but have difficulties getting close enough due to the blockage of vehicles and bystanders.	• Responders have difficulties getting close due to blockage of vehicles and bystanders. • …

Example: Staff overload can prevent issuing WEA alert

Figure 19: A Mission Thread Identifies an Operational Challenge to WEA

We performed two one-day MTWs with EMAs in two different U.S. states. Both were hosted by counties but included state and municipal participants. Table 5 provides some high-level statistics about the number of participants and the EMAs that they represented. We include detailed results from these MTWs in Appendix D.

Table 5: EMAs That Participated in MTWs

Characteristic	Organization A	Organization B
Geographic size	1,778 square miles	778 square miles
Population (from 2010 U.S. census)	4.1 million	534,543
Number of MTW participants	10	11

In our sessions, we focused the mission threads on analyzing the impact of incorporating WEA into existing processes. We found that the MTW was useful in helping EMAs reason about the impact of WEA on their operational procedures. EMAs can then use the output from the workshop to update operational procedures, system test cases, drills, exercises, plans, and so forth. We found that the MTW method systematizes the tabletop exercises that many EMAs already use. The EMA participants said they would be comfortable conducting their own MTW or similar event to understand other challenges and to develop guidelines for how to address them.

Observation 2: EMAs recognize the need to address and manage operational challenges prior to an emergency incident.

Based on our mission thread analysis of these two different MTWs, each of which involved several EMAs, we observed some common themes. In Table 6, we provide some of the specific concerns from Organizations A and B, and then we summarize some of the common themes (the entire mission thread results can be found in Appendix D).

Table 6: Common Concerns of EMAs About WEA

Common Theme	Organization A Concern	Organization B Concern
1. EMAs are uncertain about when it is appropriate to send a WEA message (vs. using another type of alert or warning channel).	What civil emergencies are worthy of a WEA message?	When does an emergency warrant transmission of a WEA message?
2. EMAs do not always incorporate cybersecurity practices into systems and operations.	From a security perspective, is the EMA handling information during alerting operations in an appropriate way to support its mission?	How should the EMA incorporate cybersecurity into its operational and support procedures?
3. EMAs lack certainty about anticipated call volumes and have concerns about whether infrastructure will satisfy demands.	Does the EMA's infrastructure support the anticipated volume of requests for additional information via phone, email, and website channels in response to issuing a WEA message?	How can the EMA handle the volume of incoming 911 calls during an emergency and simultaneously provide timely alert notification to the public?
4. EMAs have concerns about how to make the public aware of how to respond to alert messages.	Will the public understand and trust WEA messages?	How can we educate the public to understand WEA messages and take appropriate action?
5. EMAs have concerns about how to understand the increasingly complex systems and how technology will evolve.	How will the EMA ensure that it acquires alerting products that meet operational and sustainment needs now and in the future?	How can the EMA manage multiple input and output channels (e.g., 911 text messages, videos)?

In this section, we describe the five common themes in more detail.

EMAs are uncertain about when it is appropriate to send a WEA message. Participants at both MTWs said that they struggle to determine what types of emergency incidents warrant sending a WEA notification. EMAs understand that they should work with state, county, and local stakeholders to determine these thresholds in advance. One aspect of the complexity is that there are many possible alerting methods with different strengths. Geotargeting capability and severity of incident are key factors to consider.

Figure 20 illustrates the expected frequency of use of various alert and warning methods. It is expected that Twitter and Facebook will be used heavily, including for relatively minor incidents. Subscription emergency-notification alerts such as email, SMS, and phone calls are expected to be the next most frequently used media channels. Less frequently used are sirens, then WEA, and finally EAS. EMAs will use WEA and EAS channels only in the worst cases to inform citizens of an action that they need to perform immediately.

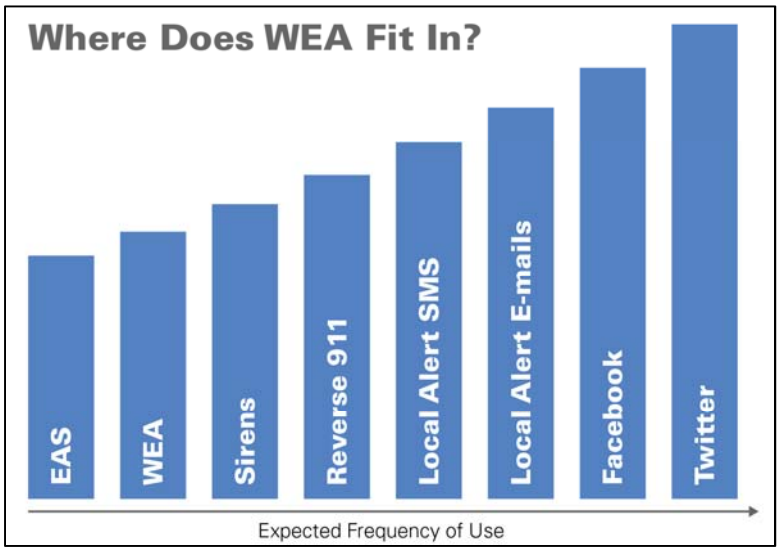


Figure 20: Hierarchy of Alerting Output Channels [Adapted from DHS S&T 2013]

EMAs do not always incorporate cybersecurity practices into systems and operations. Not only in the two MTWs we conducted, but also across the many organizations that we interviewed, we discovered a general lack of awareness of AO vulnerabilities that may enable cyber attackers to modify, delay, destroy, or spoof WEA messages. This point is addressed in Section 7 of this report and in greater detail in Section 4 and Appendix D of the *WEA Service Cybersecurity Risk Management Strategy for Alert Originators* [SEI 2013].

EMAs lack certainty about anticipated call volumes and have concerns about whether infrastructure will satisfy demands. The main concern is that infrastructure may not support the volume of requests for additional information that come in through phone lines, email, and website channels in response to a transmitted WEA message. Because of the WEA message's 90-character limit, EMAs expect to receive more phone calls requesting additional information compared to other notification methods that allow for longer messages. Once an EMA broadcasts a WEA message, media entities and PSAPs realize that they should be prepared for the increase in public requests for more information.

EMAs have concerns about making the public aware of how to respond to brief alert messages. Another concern that MTW participants raised is that the public is not well informed about WEA. People might not trust the message and might ignore it.

EMAs have concerns about how to understand the increasingly complex systems and how technology will evolve. Due to the complexity of information flow and the systems involved in emergency management, it is becoming more difficult to have a solid understanding of operational and sustainment needs now and in the future.

Observation 3: There are existing practices that can assist EMAs in sending rapid, clear, and timely messages during an emergency.

We observed a number of practices that EMAs found useful for enabling rapid alerting during an emergency.

Using message templates. Several organizations we interviewed have developed templates that they can use to create messages quickly and easily. The alerting community has long used this practice, and organizations considering sending WEA messages are already thinking about carrying over this practice. Templates will also help EMAs to develop messages that stay within the 90-character limit. In addition, EMAs can use templates to generate messages in languages other than English and vet them with appropriate citizens in advance.

Creating complete alert messages. To learn how to create good alert messages, AOs can take FEMA's independent study course "IS-247.A: Integrated Public Alert and Warning System (IPAWS)" [FEMA 2012b]. This course suggests that alert messages should possess five research-supported attributes: messages must be clear, specific, accurate, certain, and consistent.

Using graphical user interfaces to set alert boundaries. Many EMAs preferred to use products with graphical mapping capabilities over strictly text-based alerting products. While a graphical mapping interface enables ease of operation, it presents a challenge with WEA because WEA disseminates by county code. This graphical mapping capability could be misleading if implemented in a vendor product because the message might go beyond the boundary shown on the screen (when compared to the other alerting-notification tools EMAs may use that have more granular options for choosing the dissemination area). Future versions of IPAWS and WEA may allow for more narrowly defined targets using geospatial coordinates (i.e., latitude and longitude). We observed that many EMAs are reluctant to issue WEA messages until they can target messages more narrowly.

Observation 4: Large-scale exercises and training are important to exercise cross-agency and cross-system scenarios.

Many EMAs participate in cross-agency, large-scale exercises in addition to drilling. Many stakeholders that we interviewed mentioned having or wanting to have regular training for the operators to practice sending WEA messages. Exercises are commonplace in the EMA community. These exercises vary considerably in scope, method, and expense, from short tabletop exercises to full, simulated, or role-playing events.

Observation 5: There are cross-organizational and media-channel coordination challenges in issuing WEA messages.

Cross-Organizational Coordination Challenges

In the MTWs we conducted and other stakeholder interactions, many organizations expressed concern about coordinating messaging responsibility among overlapping alerting jurisdictions. This is particularly a problem for large counties with dense populations and multiple municipalities. At this early stage of WEA adoption, we found a lack of defined protocols and agreements among organizations at the state, county, and local levels about who would issue alerts and when. Due to the distributed nature of the WEA service, lack of coordination such as this can result in undesired outcomes. We illustrate this challenge using two examples from our stakeholder interactions.

Example 1: A local emergency occurs (such as a chemical spill) in a large county jurisdiction. The local EMA sends an alert telling people to evacuate. The county EMA also sends an alert

with conflicting information, such as instructions to shelter in place. The public is confused about how to react; some take action and some don't.

Example 2: An EMA requests the National Center for Missing & Exploited Children (NCMEC) to send an AMBER Alert. NCMEC and the individual EMA do not coordinate on timing for the notification. NCMEC sends the alert without notifying the individual EMA. The WEA AMBER message quickly goes out across many jurisdictions. However, the local communities are not ready to support the alert with synchronized information. When message recipients try to get more information, none is available, so the EMA loses an opportunity to engage more people in a search at the local level.

Media Channel Synchronization Challenges

We also observed, through stakeholder interactions, the potential for conflicting messages among EMAs and media outlets used to warn the public. The problem is that, unlike in previous alerting contexts where channels were limited primarily to television and radio broadcast, web-based channels blur the boundaries of the media market. People can access websites from anywhere, and there are many more channels to keep synchronized. EMAs will need to deal with increasing complexity as they coordinate all of these channels. From an operational perspective, EMAs said that they need to develop organizational protocols and procedures capable of dealing with this complexity.

WEA messages are intended to be an initial warning and, therefore, alternative distribution paths must be in place to supply additional information. Ideally, these channels will be coordinated and synchronized, particularly during a disaster. The potentially contradictory instructions in Example 1 illustrate a situation in which synchronization does not happen. However, Figure 21 illustrates an example where the problem is more complex because of the addition of uncoordinated communications channels that may or may not be controlled by official agencies.

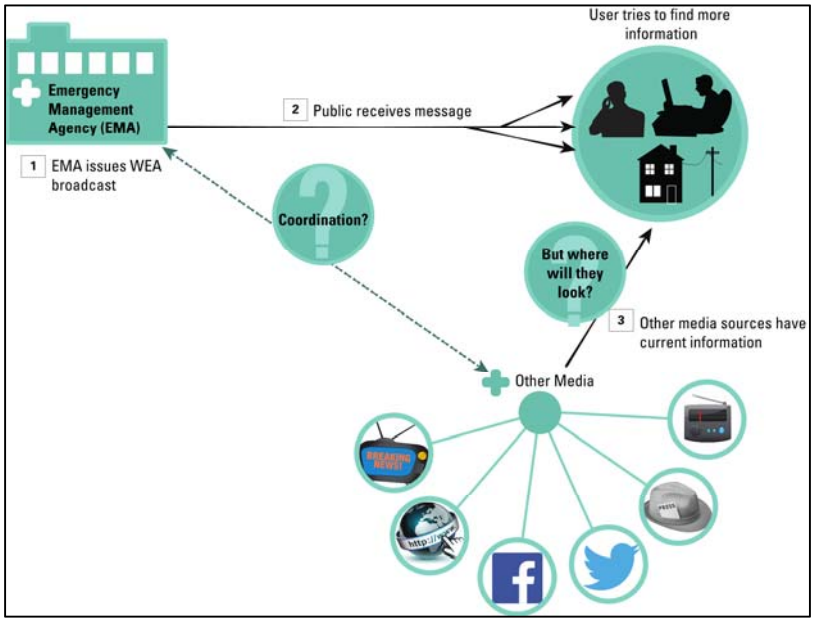


Figure 21: Coordinating Emergency Information Among Media Channels

10.2 Recommendations

We make the following suggestions for addressing cross-organizational and media-channel synchronization challenges.

Determine how to manage operational challenges before an emergency event occurs.

- Develop civil emergency scenarios for when and how to generate WEA messages, and include these in emergency-management strategic plans. Make sure that scenarios address distribution and coordination of messages across multiple channels.
- Develop a communication plan that details with whom to coordinate during an emergency and how to do it.
- Look to NWS, FEMA, DHS, and states for lessons learned and best-practice guidance regarding alert decision making.
- Conduct detailed planning and coordination so that all stakeholders understand and accept the final procedures for your alerting hierarchy.

Prepare the public to respond appropriately to WEA messages.

- Perform public-awareness outreach activities through many communications channels to educate citizens about WEA. Some organizations target television, radio, and utility bills and stay alert for creative communications opportunities.
- Work with vendors to capitalize on their knowledge of how the public actually uses their products in an emergency event. For example, analysis of communications traffic could identify issues and suggest possible solutions.

Continue learning about alerting capabilities as technology evolves.

- Periodically meet with the vendor providing WEA capability to gather current information, document lessons learned, and understand new and planned features for the product. Several vendors we talked to would welcome this opportunity to improve their products.
- Periodically meet with CMSPs in your area to understand current and planned WEA capabilities and geotargeting coverage such as FIPS code, polygon, and circle. Infrastructure on the disseminator side also influences WEA implementation. The penetration of cell towers, current capabilities, and upkeep as well as planning for future capabilities and maintenance can affect the delivery and response to the WEA message. Communicate with your local CMSPs to understand the capabilities and support for WEA messages that their switches provide. Ask CMSPs when they update their gear both at the switch level and at the cell tower. This is changing as CMSPs roll out new networks (e.g., 4G/LTE networks).
- See Appendix G for a list of useful resources on a variety of topics, including alert types, alerting authority, developer information, public outreach, tools, and standards.

Perform interagency training, drilling, and exercises to plan for coordinating across jurisdictions during an emergency.

Conduct training, drilling, and exercises on a regularly scheduled basis. A key reason for interagency training and drilling is to develop coordination and validate processes and procedures. In addition, cross-organizational exercises help identify potential failure points with supporting tools and technologies. Some examples of analysis methods that EMAs can apply in this context in-

clude the MTW and the RACI method. We briefly describe these methods here and provide more detail in Appendix D.

We used two analysis methods for this study that EMAs can also leverage to reason about these challenges:

- **The Mission Thread Workshop (MTW).** We successfully used the MTW to identify cross-jurisdictional issues (see Appendices C and D). The MTW is a facilitated workshop useful for large-scale, cross-agency systems and missions that generates procedural and technical risks as output. The MTW proved useful in identifying common themes faced by EMAs and enabled them to articulate their challenges to gain insight into their emergency-management systems and how they interact. We recommend that EMAs use this or a similar method because the first step of solving these issues is to identify them. Participants at these workshops concurred that this was a useful method.
- **The RACI method.** The RACI method is an approach used in industry and government that helps to rapidly identify risk areas for responsibility coordination and to clarify roles and responsibilities for the future. The RACI method identifies roles and responsibilities as follows: R = responsible, A = accountable, C = consulted, and I = informed [PMI 2009].When two or more organizations need to work closely together to resolve coordination conflicts at the detailed task level, a RACI session could be a useful analysis method. In part of an MTW, participants successfully applied this method. Figure 22 illustrates its use. Across the top of the matrix are stakeholders. Down the left side are tasks that stakeholders need to execute successfully to send a WEA message. The values inside the matrix represent roles and levels of responsibility. The example matrix illustrates a situation in which multiple stakeholders believe that they are responsible for sending an alert, and no stakeholder believes that he or she has the task of coordinating with other jurisdictions about who should send alerts and in what circumstances. This highlights areas where the responsibilities need clarification. The group can refine the chart further once the organizations agree on division of responsibilities.

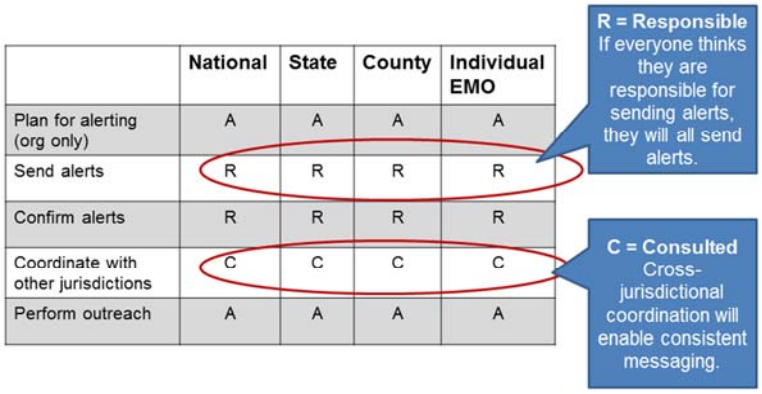


Figure 22: The RACI Method

Work with other EMAs, the media, and the public to synchronize WEA information with other media channels.

Educate the public. The EMAs involved in our study stressed the need to educate the public. FEMA emphasizes that EMAs should use WEA messages as initial notification, not as the source for continuing information about an incident. As people try to reach friends and family out of

concern for their safety, public demand on the cell phone networks far exceeds capacity and these services become inundated. EMAs should teach the public in their jurisdictions which media channels to turn to for more information.

Leverage modern media channels. EMAs in our study also emphasized the need to coordinate with web-based media channels, particularly community websites and social-media outlets. Web-based media channels can act as extensions of the individual EMA's emergency-management system, which now includes elements that it directly controls (its own solutions) and elements that it does not directly control (e.g., web-based media channels). To relieve pressure on cell service, EMAs might also encourage the public to use Wi-Fi hotspots instead of cellular coverage to ease pressure on cell phone providers during peak load.

Emulate model organizations. EMAs can also look to experienced organizations with successful media-coordination practices as models. For example, NWS offers the StormReady program to local communities. It includes information and guidance on establishing a 24-hour warning point and operations center and setting up a community emergency-response center. The goal of the program, as stated on the National Oceanic and Atmospheric Administration (NOAA) StormReady website, is "StormReady … helps arm America's communities with the communication and safety skills needed to save lives and property—before and during the event. StormReady helps community leaders and emergency managers strengthen local safety programs" [NOAA 2013]. Even if communities don't want to join the program, they can learn from how the participants operate.

Based on the response during the Boston Marathon bombing in April 2013, we also add the Massachusetts Emergency Management Agency (MEMA) to the list of model organizations for media coordination. MEMA leveraged several media channels during the event, even using Twitter to get the word out that it had issued a WEA message. *Emergency Management Magazine*'s "Alerts & Notifications" blog posted an entry about MEMA just days after the attack:

> *The best examples of best practices often come from real life. MEMA showed the rest of us strong best practices when they issued the shelter-in-place order last week. MEMA used the new broadcast cell system, Wireless Emergency Alerts (WEA), to help spread the word. That's exactly the type of event, an imminent threat, WEA was intended for.*
>
> *But, MEMA took the WEA message further. They clearly showed us how WEA can work with other media. As they issued the shelter-in-place alert via WEA, they also sent an advisory in advance to media to make sure media knew that WEA was about to be used. It's possible this was the first time some people in the media had heard of WEA (formerly Commercial Mobile Alert System)... Because of the MEMA media advisory, local media could help the public understand who was sending these unusual messages to their cell phones, and why.*
>
> *Then, MEMA Tweeted to its followers that the WEA message was issued. The Tweet was then re-tweeted, some people referring to WEA as a "phone siren." [Wimberly 2013]*

Assign a media coordinator. Many EMAs assign someone the explicit role of media coordinator. Stakeholders have considered this a natural extension to the public information officer role. The media coordinator should define media-coordination procedures and practices for the EMA. Then the EMA should exercise these media-coordination procedures regularly during emergency-response drills and end-to-end emergency-warning system tests. The media-coordinator role typi-

cally includes a community outreach and education component. The media coordinator should maintain contact with public media channels during an emergency.

11 Alternatives to Buying a WEA Solution and Associated Considerations

11.1 Observations

This section is aimed at EMAs that are considering alternatives to buying a vendor product to send WEA messages. In the first observation, we note that many EMAs see only two options: build or buy. However, we observed a few more. We introduce these options and provide a summary table of advantages and disadvantages. In the second observation, we share some of the challenges that organizations that have developed their own solutions encountered in the area of authentication and message validation. In the third observation, we describe considerations for error handling.

Observation 1: EMAs have several options for obtaining a WEA solution, and they each have advantages and disadvantages.

Through interviews, we observed that EMAs currently lean strongly toward purchasing packaged alerting-solution software products instead of developing their own alerting software. Only the national-level organizations such as NWS or NCMEC appear to be building their own solutions. However, several large-scale EMAs said that they would consider building their own alerting solution in the future. They stated that this is primarily due to the lack of control that results from depending on vendor-managed and -maintained products for alerting capability (e.g., unexpected upgrades, delays getting custom features developed). EMAs generally consider two development and acquisition strategy options: building and buying alerting software solutions. However, these are not the only options that EMAs should consider. To assist those EMAs making these decisions, we summarize and compare the following options:

- Buy software
- Subscribe to service
- Share a warning center
- Build in-house
- Leverage open source

Option 1: Buy a software package. A number of vendors offer software packages that can originate WEA and other alerts. In some cases these products are dedicated warning solutions, and in others the warning function is an additional feature in an emergency-management software suite. Many of these products can also control local warning systems such as sirens or telephone notification from the same CAP alert message. Financial, technical, training, and support arrangements for purchased products vary widely depending on the vendor, contract negotiated, and product capabilities. Demands placed on EMA IT and network facilities and staff may also vary widely, depending on the contractual agreement. Some EMAs that we interviewed expressed concern about the cost of changing software vendors, particularly in cases where the product has been highly customized or integrated with other emergency-management products.

Option 2: Subscribe to a remotely hosted commercial service. A common alternative to implementing commercial alerting software on site is to subscribe to a remotely hosted service ac-

cessed via the internet or over a dedicated data network (discussed in Section 6). This approach is referred to as a cloud-based SaaS. These applications also range from highly specialized warning solutions to broadly integrated emergency-management packages.

SaaS-based approaches can reduce financial costs in a number of ways. Providers can amortize equipment and maintenance costs across a large number of customers. And EMAs can minimize on-site equipment costs and maintenance costs. If the remotely hosted solution is not highly customized, the cost of changing to another SaaS vendor product if the EMA is dissatisfied may be less than with Option 1. Setup may involve a few simple steps to connect to the solution through a web-based URL and set up user accounts, assuming that the vendor has an established memorandum of agreement (MOA) and FEMA approval to send WEA messages. Users of some widely used vendor products reported a sense of community and safety in numbers. These vendors keep up with evolving WEA interface standards and new testing protocols and options, and they provide a forum for sharing information. However, a drawback to relying on vendors for such information is that they may not be highly motivated to provide current information on WEA capability because they also offer similar capability.

Option 3: Participate in a shared warning center. Many agencies and jurisdictions plan to issue relatively few public alerts. As a result, they have difficulty justifying investment in warning software, training, and alerting-related exercises. They also have concerns about issuing public warnings with little training or experience with alerting. Not infrequently this leads to uncertainty and anxiety that can delay or even inhibit prompt and effective use of available warning capabilities such as WEA.

California's Contra Costa County Community Warning System (CWS) has demonstrated an innovative alternative that forms the basis of the 2012–2017 Bay Area Urban Areas Security Initiative (UASI) strategic plan for public warning [Bay Area UASI 2012]. Instead of duplicating training and facilities in dozens of agencies, the Contra Costa system provides a single specialized warning center for all jurisdictions and agencies in the county. CWS operators are highly trained in public warning systems and practices and are on call 24/7 to attach as technical specialists to Incident Commands countywide in accordance with NIMS and the California Standardized Emergency Management System [Cal EMA 2011, FEMA 2013d]. This approach greatly reduces investment in equipment, software, and training. It also minimizes switching costs when changes are required, as the number of operators who need to be retrained is minimized. With over a decade of experience, the CWS warning capabilities are enhanced and streamlined. EMAs that share the warning services benefit from improved geotargeting capabilities and an increased likelihood that timely, targeted warnings will be sent when the need arises.

This approach requires a high level of interagency cooperation and embracing of an integrated, all-hazard, multimedia approach to public warning. This paradigm shift is inherent in IPAWS and CAP-based alerting generally, but it will take time for "warning mutual aid" to become familiar to emergency managers who historically have been trained to approach warning as a disjoint patchwork of hazard-specific and agency-specific systems.

Option 4: Build in-house. EMAs can achieve the highest level of control and customization by developing an in-house hardware and software solution. Custom development permits stronger control over feature development, system performance, release schedules for changes, as well as documentation and training. Developing an in-house alerting solution may be particularly attrac-

tive if the EMA desires to integrate the warning capability into a suite of emergency management solutions and capabilities. These may include integration with computer-aided dispatch or geographic information systems. But relatively few agencies have the technical and financial resources to develop and maintain their own custom-warning software packages. We provide an extended discussion of development considerations in the rest of this section.

Option 5: Leverage open-source software. Open-source software can be an attractive compromise between full in-house development and becoming locked in to a commercial product or service. It is typically free and comes with the source code needed to adapt it to users' needs [Riehle 2007]. There is at least one open-source software package being developed for CAP alert origination for which the IPAWS certification process is already underway.[8]

Open source is generally not a "turnkey" option for CAP implementation, but for agencies that have some access to IT skills and cannot justify a full in-house development effort, it may prove a cost-effective alternative.

Table 7 summarizes several advantages and disadvantages for each option. To be clear, these are generalized advantages and disadvantages, so whether or not they apply to an individual organization depends on its specific circumstances.

Table 7: Summary of Options for Obtaining a WEA Solution

Option	Advantages	Disadvantages
Buy software	• Defined procurement process (either already have or can get advice from other EMAs) • Vendor performance criteria can be specified in warranty • Design informed by developer's experience • Software developers are dedicated to the product or vendor • Clear responsibility for training and support (if specified in contract) • Collective input on design from multiple organizations in marketplace • Potentially higher quality because commercial products tend to be heavily tested	• Loss of control over customized features and integration • Features may not be ideal for any single user • Integration into existing alerting systems and operations may be awkward • Customizations may be expensive • Future cost of switching to a different solution can be relatively high if solutions are heavily integrated • Risk of vendor changing focus or going out of business • Upgrade and maintenance cycles may not align with organization's needs
Subscribe to a remotely hosted service	• Simple service contract • Minimal in-house support required • Performance can be specified in contract • Design reflects sum of all subscribers' requirements • Sustained relationship for training and support • Cost of enhancements shared across entire subscriber base	• Features may reflect "least common denominator" across potential market • Customization may be expensive or not possible • Provider can impose changes on its schedule • Risk of provider changing focus or going out of business

[8] At Carnegie Mellon University, Silicon Valley, as part of its Disaster Management Initiative (http://sv.cmu.edu/dmi).

Option	Advantages	Disadvantages
Share a warning center	• Lower cost or free • Economies of scale by minimizing duplication in staffing, training, and technology procurement • Specialist warning staff can be highly trained and experienced • Costs of making changes in the future are minimized; market power of agencies is maximized	• Requires coordination of policies and practices across participating jurisdictions • Some minimal size of service area required to justify specialist staffing
Build in-house	• EMA has maximum control over features, technical specifications, training, and maintenance • Design can be tailored to the needs of the organization, including local policies and practices • Can leverage existing expertise solutions, software, and environment • Warning functions can be integrated into dispatch, Geographic Information System, and other in-house systems • Familiarity with existing software architecture and dependencies • Visibility and understanding of the quality of the system and its code • Incentive to keep up with WEA interface-related and other evolving information	• Need for IT staff with appropriate expertise in software development and maintenance • EMA absorbs all risks of budget, technical development, and maintenance • Quality determined by individual EMA's resources • Future switching costs may include intra- or interagency budget impacts
Leverage open source (variant of build)	• Minimum expense for basic software • Can "bootstrap" local customization based on an available source code • Community of users share upgrades and bug fixes, and sustain product even if original developers disengage	• Requires some in-house IT expertise to implement • Training materials and documentation may be uneven in quality • May encounter reluctance from IT or procurement staff not familiar with open source

Observation 2: There are special considerations for developing your own WEA solution.

In some cases, we observed that EMAs would like to consider developing their own solutions; however, they don't have enough information about the cost and effort required to do so. For example, we met with a very large county-level EMA. The head of the EMA stated that he would like to build and maintain his own alerting solution sometime in the future because the organization would like to have better control over customizing the solution and improving responsiveness to software changes than they have with the current vendor-supported option. He would like to have his own development staff, locally host the solution, and provide all training and support on premise.

This sounds very tempting, especially if an organization has a great deal of emergency-management responsibility, many users, and evolving needs. However, there are several aspects to consider that may not be clear to someone who is not in the software or system-development field. In this section, we cover several considerations related to this example.

Additional infrastructure. Generally the EMAs we spoke with realize that if they build their own solutions, they will need to host the production servers and network resources required to

send a WEA message. However, systems and software engineering best practice suggests that testing and development activities be conducted in an environment physically separate from the live system. This means that an EMA might need to purchase additional hardware infrastructure to mimic the production environment. The portion of Figure 23 within the dashed rectangle shows the live production environment in which alert messages (CAP-formatted XML documents) are sent to IPAWS-OPEN for dissemination. The red circle in the bottom portion of the figure illustrates the possible need for additional infrastructure and tools. In addition, the EMA may need to purchase tools to support development and testing of the alerting software such as

- source-code editor
- compiler and debugger for the language in which the web client will be developed
- tools for processing XML (e.g., XML editors, schema generators, and schema validators)
- software testing tools, including CAP message syntactic and semantic testing tools, defect-tracking tools, and automated testing tools
- configuration-management tool

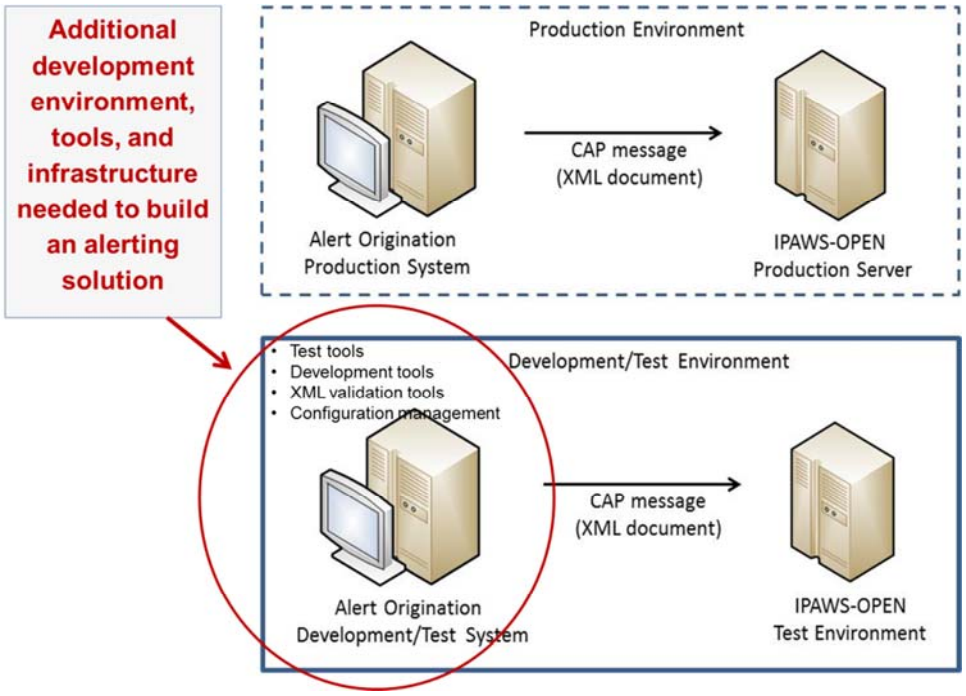


Figure 23: System Development and Production Environments

Technical expertise. In our example, the EMA clearly hoped to leverage development expertise for several projects. The EMA would develop the software using whatever programming language and tools are compatible with the existing environment. However, in addition to needing the experience to develop software using its own tools, the development team requires expertise in developing XML-based, web-based systems. Not only should the developer have expertise in the web client's implementation language (e.g., Java, C++), a developer of a WEA capability should also have experience in

- XML, required to create a message for consumption by IPAWS-OPEN [W3C 2008a]
- the XML-based CAP 1.2 standard [OASIS 2010]
- the IPAWS-OPEN CAP profile [OASIS 2009]

- XML digital signature processing, required to sign the message and package it for sending to IPAWS-OPEN [W3C 2008b]
- SOAP[9] [W3C 2007a]
- WS-Security [OASIS 2004]
- Web Services Description Language (WSDL), required to understand the service interfaces provided by IPAWS-OPEN [W3C 2007b]

If an AO also wishes to exchange information via the COG-to-COG messaging capability provided by IPAWS-OPEN, then the developer will need additional expertise in EDXL-DE [OASIS 2006]. EDXL provides a message-routing mechanism and can act as a message envelope for CAP content exchanged between EMAs. CAP also has message-routing information, but EDXL may be more suitable for COG-to-COG communications because it can include additional media elements—such as audio or video files—not present in the basic alert.

System and software design considerations. According to the EMAs and vendors we spoke with, successfully formatting and sending a WEA message is not challenging. If a development team follows the FEMA developer materials, it should be able to develop that functionality rather quickly. However, beyond the basic functional requirements, there are also quality attribute (non-functional) requirements such as performance, security, and availability requirements that EMAs need to consider. These typically require integrated design for software and hardware infrastructure components.

In addition, stakeholders for the new system can quickly pile on functional requirements. For example, most of the EMAs we spoke with would like to integrate their alerting solution with incident-management solutions. The users may also want to integrate a complex graphical-mapping capability, a communication portal, predefined message templates, situational awareness, or other capabilities found in vendor products. Looking to the future, users may want to access the alerting solutions from their own mobile devices. Thus, the path to in-house development of a WEA solution may lead to a larger development effort than originally envisioned.

Observation 3: There are important considerations related to authentication and message validation.

When we interviewed organizations that had developed their own software and sent WEA messages, we asked them what types of challenges they encountered as they developed their solutions. The general consensus was that the IPAWS-OPEN SOAP-based interface and CAP standard are well documented and fairly easy to master. However, in any system interaction between independently operated and governed systems, changes on either side can break the interaction. Even with well-defined interfaces and standards, problems can arise due to mismatched expectations regarding functionality, policy implementation, and syntactic and semantic interoperability assumptions [Lewis 2012]. Organizations that we spoke with described two areas where they experienced minor challenges during development and testing. These may be areas where organizations considering developing their own solution might carefully examine the documentation and be prepared to reach out to FEMA if they run into trouble. These areas are

[9] Formerly "Simple Object Access Protocol."

- security-certificate authentication setup and management
- XML-validation assumption mismatch

The EMA's developers should prepare to handle challenges related to security-certificate authentication. The SOAP envelope and the alert message must have a valid digital signature so that FEMA can authenticate the sender (Figure 24 illustrates). FEMA provides the digital certificate required for signing messages when an organization signs an MOA to become an authorized WEA originator. Even though IPAWS-OPEN uses the WS-Security standard, implementers still make many decisions when they implement authentication (e.g., types of tokens to use, digital signature, and encryption). This means that the alerting organization should understand not only what the authentication service requires but also what IPAWS-OPEN expects for authentication validation. One organization we spoke with had problems with certificate authentication during testing. Fortunately, they easily resolved this with help from FEMA.

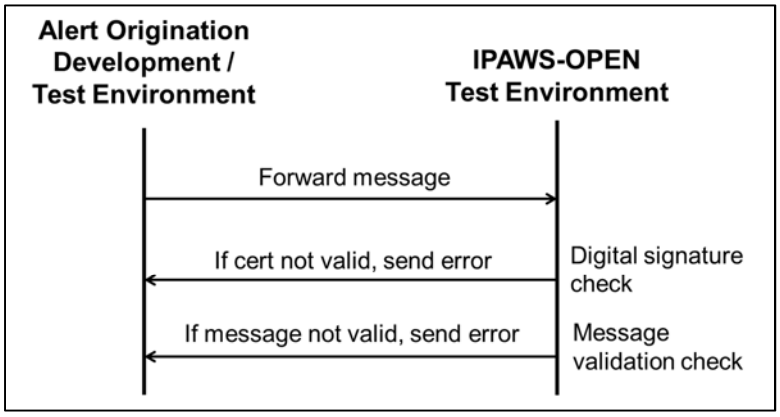


Figure 24: Security Certificate Authentication

In addition, the AO must securely maintain and manage the required security certificates. For example, the EMA needs to request and import new certificates when the old ones expire. If you have a vendor product, the vendor will probably take care of this for you. If you develop a solution yourself, then certificate management is the EMA's responsibility and you should assign this activity to someone within the organization. We suggest periodic testing of certificate validation at the individual user level—system administrator testing is not enough. If an emergency arises and someone logs on with permission to send an alert, IPAWS-OPEN will reject the message if the certification is not properly imported or has expired. An emergency event is not the time to find out that user authentication is not working.

The EMA's developers should also prepare to handle challenges related to the XML-validation assumption mismatch. To understand this issue, EMAs need to understand how the messaging works. Client–server interactions between an alert-origination system and IPAWS-OPEN consist of exchanges of messages that are constructed as documents written in XML. The client sends service requests in the form of messages to the IPAWS-OPEN server. IPAWS-OPEN validates the message and takes appropriate action based on the message contents. The IPAWS Alert Aggregator service ensures that all messages are correctly constructed according to the CAP standard and the IPAWS-OPEN profile. The CAP standard specifies how to structure an XML document as a CAP alert message, and the IPAWS-OPEN CAP profile is an interpretation of the CAP standard to apply to the message so that it meets the IPAWS requirements. When an EMA sends

an alert message, the alert-origination client sends the message to the correct service interface of the IPAWS-OPEN server by wrapping the message in a SOAP envelope (XML based) and transmitting it via HTTPS over a secure internet connection.

One organization described an incident in which it had built the message according to the specifications; however, IPAWS-OPEN repeatedly responded with an error message that the XML validation step had failed (the bottom-most error path shown in Figure 24). After some investigation, FEMA identified the validation error and made a correction. Again, the organization reached out to FEMA quickly to resolve the issue and found FEMA extremely responsive and helpful in addressing the problem.

Observation 4: There are challenges with error-handling message propagation.

Some of the development experiences that we captured came from vendors, since they have been the most active in developing their own alerting software. Their experiences are clearly applicable to those considering developing alerting solutions themselves, as they will likely run into the same challenges. One vendor described an interesting challenge related to error handling and processing of error messages generated by IPAWS-OPEN. In this example, the organization developed software and deployed the software package to the users for an EMA. The solution has the capability to capture and display error messages returned by IPAWS-OPEN. In this case, a user sent a test message, received a cryptic error message from IPAWS-OPEN, and was not sure what to do next. The administrator could not see the error message. This suggests that EMAs that develop their own solutions need to be aware of the error responses that can come from IPAWS-OPEN and propagate them beyond the user to the administrator so that the development team can address the problem.

11.2 Recommendations

Understand the advantages and disadvantages of each build-your-own option so that you can make an informed choice.

- Make an informed choice by interpreting the options in light of the organization's specific circumstances and requirements.
- Look beyond the desired alerting capabilities; you should also consider training, maintenance, and total cost of ownership.

If you choose to build in-house, then

- conduct development and testing in an environment separate from the production alerting system
- look beyond the desired functionality and consider issues such as system performance, security, and availability
- pay particular attention to authentication, message validation, and error handling

Keep Current with Evolving Standards

For organizations that decide to develop their own alerting capabilities, there are a couple of key sources of information. The first is FEMA's IPAWS program. FEMA has provided guidance for the construction of CAP messages and the development of IPAWS-OPEN web-service clients.

The second is OASIS, which is the official standards organization that develops and releases new CAP standards. Documents from these key sources include

- CAP standard [OASIS 2010]
- IPAWS profile [OASIS 2009]
- Web-service interface design guidance [FEMA 2013c]

For information about OASIS, visit the society's website at www.oasis-open.org; for information on CAP, see www.oasis-open.org/standards. Another good CAP source is a wiki under development called the CAP Cookbook. Information about it can be found at https://lists.oasis-open.org/archives/emergency/200507/msg00010.html. FEMA also maintains an active web presence for IPAWS. FEMA conducts scheduled developer webinars that cover a wide range of relevant and helpful topics. These materials can be found on the FEMA IPAWS website: www.fema.gov/integrated-public-alert-warning-system.

12 Conclusion

12.1 Summary

This report represents the results of a study of WEA adoption issues. We acknowledge nearly 50 organizations for making significant contributions to the data-collection phase of this project. We gathered data through artifact review and interviews with EMAs, vendors, and experts in the emergency-alerting field. We also conducted two one-day Mission Thread Workshops hosted by Harris County, Texas, and Jefferson County, Colorado. We analyzed the data and allocated observations to 10 key areas of concern for WEA adoption by EMAs.

A significant finding was a general lack of awareness of AO vulnerabilities that may enable cyber attacks on WEA messages. We refer the reader to Sections 3–6 of the *WEA Service Cybersecurity Risk Management Strategy for Alert Originators*, which focuses on these threats and the application of a cybersecurity risk-management strategy [SEI 2013].

Another significant finding was the importance of EMAs' understanding and specifying requirements for WEA services. Requirements are essential to get right because they drive everything from product selection, to integration decisions, to implementation, to definition of test cases. By properly specifying key functional and quality attribute requirements, EMAs can have much more confidence that the systems will meet their demands.

Finally, this study demonstrated the value of scenario-driven discussions among stakeholders. The SEI's Mission Thread Workshop proved useful in identifying WEA adoption and integration issues.

12.2 Future Directions and Next Steps for WEA Research

As of this writing, the WEA service has been in operation since April 2012, or a little more than a year. It will take time for public alerting practices to fully incorporate new paradigms and new solutions such as the WEA service. Its innovative nature and interdependency with the now-ubiquitous wireless technology make it a greenfield for multiple research directions. We present three initial examples of study and research directions to maximize the public benefit of the WEA service in the future.

Simultaneous and consistent use of multiple alert-delivery mechanisms. Instead of building a patchwork of specialized alerting systems that address particular hazards or particular technologies, modern public-warning practices stress the simultaneous and consistent use of multiple alert-delivery mechanisms. Early reports on the WEA service use by the Massachusetts Emergency Management Agency (MEMA) in the aftermath of the Boston Marathon bombings of April 15, 2013, suggest that MEMA officials took care to create context for WEA messages, for example, by issuing Twitter messages that directed recipients to additional information about the new system [Wimberly 2013].

However, this multimodal alert environment requires successful interaction of unlikely elements such as technical integration, governance of alert criteria and resources, jurisdictional infrastructure, and public education. Research into the positive and negative impacts of these key elements,

both as single entities and in combination with one or more other elements, can advance both WEA progress and the overall alerting environment.

WEA post-alert impact across other emergency services. The minimal content of WEA messages and the gross granularity of geotargeting have led to speculation that a WEA message could trigger increased voice or internet traffic, and perhaps gridlock. As the use of the WEA service increases, there will be opportunities to gather factual data on the size of the impact, if any; the distribution of the impact (e.g., 911, local media, emails, text messages); and the causes. Controlled testing of character-limit changes could support or refute a hypothesis that the 90-character limit accounts for the impact. Comparisons of the post-alert effects of geotarget coverage at the FIPS code level versus a more granular polygon approach could yield objective recommendations for technical changes.

Continual WEA technical improvement in an evolving infrastructure. The current design of the WEA service was developed in 2006 and 2007 in a process of consultation among industry and public safety and policy entities. Since that time, the nation's wireless telecommunications infrastructure has evolved and smartphones have greatly increased onboard computing power and rich user-interface features. At the same time, these increases in power and features challenge existing wireless infrastructure capabilities. As infrastructure enhancements develop to meet these demands, researchers can look more closely at modifying or expanding the technical capabilities of the WEA service.

Appendix A Data Collection and Research Methodology

We used a qualitative research approach in this study. This decision influenced several important research-design considerations including sample size, interview-pool makeup, and interview breadth versus depth, so we will briefly revisit some differences between qualitative and quantitative research. Qualitative research is particularly useful when researchers wish to avoid presupposing the expected research outcome (such as when working with a hypothesis). Qualitative researchers generally ask broad questions and collect data, typically through interviews and case studies, with a goal of understanding the themes and patterns that emerge from descriptions of actual experiences. An example of a qualitative research output derived from this study is the set of challenges revealed by the interview data. The validity of qualitative research comes from the quality of the interview data and the approach used to gather and analyze the data [Corbin 2008, Glaser 2001].

Quantitative research, on the other hand, refers to the systematic empirical investigation of social phenomena via statistical, mathematical, or computational techniques. Quantitative researchers ask specific, narrow questions or use surveys to collect numerical data [Corbin 2008]. An example of a quantitative research question in the alerting domain might be "What is the average length of time it takes to complete the FEMA MOU approval process?" We used a qualitative research approach in this study because it aligned well with our research goals. Rather than beginning the study by assuming that we knew what EMAs' biggest challenges are, we strove to identify them by immersing ourselves in the emergency-management domain to the extent possible and practical.

There are several qualitative-research approaches. We based the core of our research approach on concepts derived from a qualitative-research approach referred to as *grounded theory*. Grounded theory has increasingly been successfully applied to technical research areas such as software-development research [Adolf 2011]. As we conducted interviews, we emulated Glaser's conceptual approach to grounded theory, which aims to let the theory emerge from the data [Glaser 2001], while also leveraging some of the structured approach described by Strauss in later phases of the study [Corbin 2008]. Figure 25 depicts a high-level overview of our research process for this study. The process began with data collection and synthesis followed by identification of candidate challenges. As we continued interviews, some challenges emerged as prevalent and important to EMAs. We used the challenge information to develop recommendations for each challenge, which appear at the end of each section of this report. The parts of the process shown in gray in Figure 25 represent steps and outputs internal to the research team, and the blue shapes represent steps and outputs shared externally.

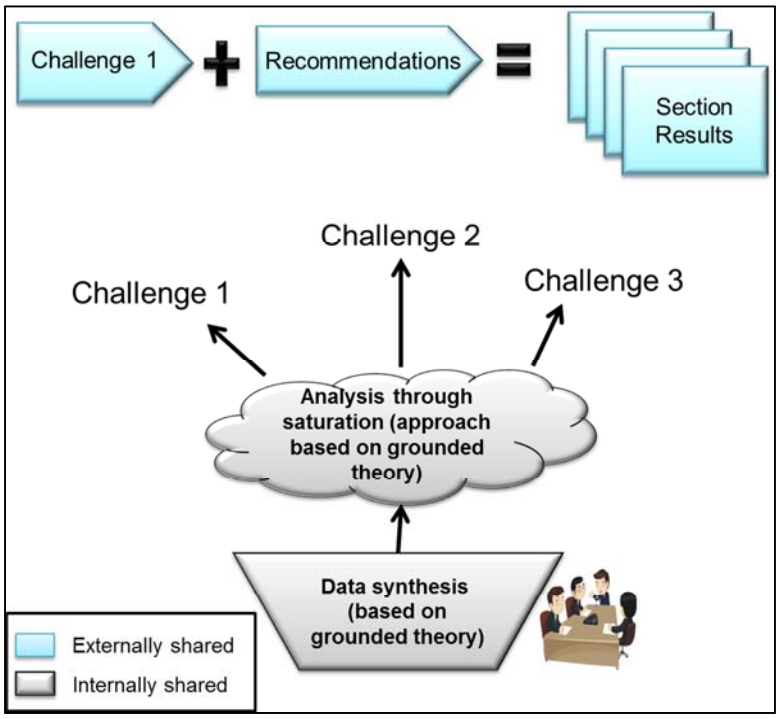


Figure 25: Qualitative Research Process for This Study

The key components of the research approach that we applied in this study include

- data collection and synthesis
- theory and challenge generation and analysis

In addition, we also conducted three small case studies. Case studies are a well-founded empirical research method, and we used them to provide an analysis framework for discussion [Yin 2002].

Data Collection

During the data-collection phase, we gathered information in several ways, including interviews with stakeholders in the field, vendors of alerting products, and other related experts as well as attendance at conferences, workshops, and webinars in the field of emergency management.

We conducted at least one interview per organization, and we often conducted multiple follow-up interviews and communicated by email with the same organization to gather additional detail and verify accuracy of the data collection and interpretation. We conducted interviews via a mix of on-site visits and teleconferences. We had the majority of interviews recorded and transcribed so that we would have an accurate copy of the data (avoiding unintentional filtering by note takers). The length of interview times varied from 60 to 180 minutes. The interviewees from each organization included technical and management staff (emergency managers, developers, and testers).

The Carnegie Mellon University Human Subject Research policy requires that we act in accordance with federal regulations, including Title 45 of the Code of Federal Regulations, Part 46, which states that we must not disclose specific information given during interviews without informed consent by people from whom we collected that information [CFR 2012a]. We promised confidentiality before all data-gathering activities. However, we summarize the organizational

characteristics of the stakeholders we interviewed in Table 8. Our research sampling covered all organization types and sizes that we targeted in our research plan.

Table 8: Summary Data of Interview Participants

Organization	Interview Date	Size/Jurisdiction	Type
Organization A	6-Apr-12	Small	Individual EMA
Organization B	21-Jun-12	Small	Individual EMA
Organization C	24-Jan-11	Small	Individual EMA
Organization D	6-Feb-12	Medium	County EMA
Organization E	31-Jan-13	Medium	County EMA
Organization F	14-Jun-12	Medium	County EMA
Organization G	13-Dec-12	Large	County EMA
Organization H	5-Jul-12	Small	State/commonwealth EMA
Organization I	26-Sep-12	Large	County EMA
Organization J	22-Jan-13	Large	State/commonwealth EMA
Organization K	29-Nov-12	Medium	County EMA
Organization L	16-Jul-12	Large	Individual EMA
Organization M	19-Jun-12	Medium	City EMA
Organization N	19-Nov-12	Small	Territory EMA
Organization O	11-Jul-12	Large	Consultant/research
Organization P	12-Dec-12	Large	County EMA
Organization Q	2-Oct-12	Large	County EMA
Organization R	11-Jan-13	Small	City EMA
Organization S	17-Dec-12	Large	County EMA
Organization T	30-Jan-13	Small	State/commonwealth EMA
Organization U	30-Jan-13	Medium	County EMA
Organization V	28-Jan-13	Large	State/commonwealth EMA
Organization W	18-Jan-13	Small	County EMA
Organization X	4-Jan-13	Medium	Individual EMA
Organization Y	31-Jan-13	Small	State/commonwealth EMA
Organization Z	22-Feb-13	Small	County EMA
Organization AA	25-Feb-13	Large	Government program
Organization AB	13-Mar-13	Large	State/commonwealth EMA
Organization AC	22-Mar-13	Medium	County EMA
Organization AD	26-Mar-13	Small	City EMA
Organization AE	1-Feb-13	Large	Consultant/research
Organization AF	29-Jun-12	Large	Vendor/service
Organization AG	3-Aug-12	Medium	Vendor/service
Organization AH	28-Jun-12	Medium	Vendor/service
Organization AI	18-Jul-12	Small	Vendor/service
Organization AJ	29-Jan-13	N/A	Consultant/research
Organization AK	20-Jul-12	Medium	Vendor/service
Organization AL	7-Aug-12	Small	Vendor/service
Organization AM	16-Jul-12	Medium	Vendor/service
Organization AN	22-Jun-12	Medium	Vendor/service
Organization AO	17-Dec-12	Large	Vendor/service
Organization AP	5-Jul-12	Large	Vendor/service
Organization AQ	2-Nov-12	Small	Vendor/service
Organization AR	18-Jul-12	Small	Vendor/service
Organization AS	12-Feb-13	Large	Vendor/service
Organization AT	14-Jun-12	Small	Vendor/service
Organization AU	9-Nov-12	N/A	Consultant/research

Organization	Interview Date	Size/Jurisdiction	Type
Organization AV	28-Mar-13	Large	Vendor/service
Organization AW	4-Feb-12	Large	Vendor/service
Organization AX	Multiple	N/A	Consultant/research

Table 9 provides a list of the conferences and other events attended by members of the research team.

Table 9: Events Attended by the Research Team

Event	Date
60th Annual International Association of Emergency Managers Conference	October 28–31, 2012
Carnegie Mellon University–Silicon Valley 3rd Annual Disaster Management Initiative Workshop	November 4, 2012
WEA demonstration in New York City, NY	December 15, 2011
CMAS Forum in conjunction with the International Wireless Communications Expo	February 21, 2012
Colorado 911 Conference	July 12–13, 2012
Homeland Infrastructure Foundation-Level Data (HIFLD) Working Group Meeting on Cyber Security and Energy Resiliency	October 3–4, 2012
International Association of Emergency Managers 60th Annual Conference & EMEX 2012	October 26–November 1, 2012
International Wireless Communications Expo	February 22, 2012
IPAWS Developer Working Group webinars	September 2012–May 2013
IPAWS Practitioner Working Group webinars	November 2012–May 2013
National Academy of Science Workshop on Geotargeted Alerts and Warnings	February 21, 2013
National Emergency Management Association Emergency Management Policy & Leadership Forum	October 8–10, 2012
National Homeland Security Conference	May 22, 2012
Organization for the Advancement of Structured Information Standards (OASIS) Emergency Alerting Policy Workshop	May 1–3, 2012
Rural Cellular Association 20th Annual Convention	September 23–26, 2012
S&T-sponsored webinar on CMAS Integration Guidance Development	July 19, 2012

Interview Question Design

The interview approach began with a broad guiding question, which is characteristic of Glaser's grounded-theory approach [Glaser 2001]. Our initial guiding question was "What are the AOs' barriers to WEA adoption and operational use (and what has gone well)?" This approach allowed for general theories to emerge without research bias. After several initial interviews, we identified a set of candidate challenge areas based on responses to our guiding question.

Once theories had emerged and we gained confidence that we were focused on the right challenges, we evolved to a probing framework of guiding questions more characteristic of Strauss [Corbin 2008]. The probing framework promoted consistent collection of detailed interview data for deeper analysis and recommendation development. Figure 26 shows an abbreviated version of the question framework.

Probing Question Framework

1. What do WEA message originators need to **plan** for to establish an operational WEA capability in their organization?
2. If **buying** a tool/service for WEA, what **product features and vendor characteristics are important** to alert originators in selecting an alerting tool?
3. If **building a capability** for sending WEA messages, what are the most **important issues** that alert originators need to consider when building an alerting tool?
4. What are the most critical **requirements** to consider with respect to a WEA capability?
5. Describe the solution design (including hosting option) and redundancy strategy.
6. How do WEA message originators make certain that their solutions are working and/or will be working when they need them (**integration and operational resiliency**)?
7. What are the most significant **cybersecurity risks** to the WEA message origination process and technologies?
8. What are some challenges of **cross-jurisdictional boundaries** with respect to planning or sending WEA messages?
9. What kinds of future changes should WEA message originators **anticipate as they design**/obtain their WEA service?
10. What other considerations should WEA message originators be aware of to support successful WEA adoption and use?

Figure 26: The Probing Question Framework for Interviews

It is important to point out that while interviewers used this question framework as a general guide, we also tailored the questions to the knowledge, background, and experience of the stakeholders participating in the interviews. In addition, the stakeholders' responses often spawned a series of unscripted sub-questions intended to gain greater understanding of the responses, and we particularly focused on gathering examples that grounded the data in real experiences.

Analysis

We analyzed the data collected during recorded interviews during the analysis step. During this step, we validated the concepts through the process of *constant comparison*, in which the analyst goes through each incident in the data and compares it to other incidents. We grouped together incidents that we found to be conceptually similar and mapped them to an emerging concept [Corbin 2008]. We continued this process until we reached saturation. *Saturation* is the process of acquiring sufficient data to develop each concept and category fully, in terms of its properties and dimensions, and to account for variation [Corbin 2008]. The goal of saturation is to gain confidence in emerging concepts and to separate weaker concepts from stronger concepts. Stronger challenge concepts became the concepts on which we centered our challenge observations.

Observations and Recommendations

Our observations include a description of the challenge as well as recommendations (as appropriate). We developed recommendations for the challenge areas primarily using WEA EMA stakeholder examples and case studies. At the time of this writing, few organizations had sent WEA

messages, so we also used analogous system experience from other domains and well-accepted reference materials to produce recommendations.

Appendix B Integration Strategy Framework

Purpose

This appendix provides a high-level view of the WEA Integration Strategy Framework for AOs. EMA staff can use this framework to reason about their adoption activities. We populated this framework with information from a variety of sources, including discussions with WEA stakeholders, information shared by other organizations that are supporting the WEA RDT&E project, and software and systems engineering best practices.

For completeness, we attempted to include in the framework all the major steps necessary for an organization to successfully adopt WEA. However, we want to make clear that the SEI is not providing guidance in all of these areas. We refer to other related materials for information, such as the FEMA website.

We describe the WEA Integration Strategy Framework for AOs using a narrative description style. We walk the reader through a scenario beginning with deciding whether to adopt WEA all the way to sustainment of WEA capability. The benefit of the narrative approach is that it allows us to describe the interplay between the management and technical activities as well as key decision points. Because this is a narrative, we do not present the information sequentially; rather, we will follow a path that alternates between the organizational and technical sides of the diagram shown in Figure 27.

To help the reader follow the narrative, we have provided circled numbers in the diagram that map to the activities described.

> For example, ① **OR-1: Establish WEA Usefulness to Organization** maps to the block on the diagram titled **Step OR-1: Establish WEA Usefulness to Organization**.

Although the numbers are sequential for the narrative, this ordering scheme is not intended to indicate that the steps are necessarily executed sequentially. For example, an organization will undertake many steps simultaneously. On the diagram, the connecting lines ending with solid circles (e.g., the connection from OR-4 to TR-1 and TR-2) represent interface relationships among the organizational and technical activities of the framework. These interfaces reflect the fact that organizational and technical staff will exchange information and collaborate on key decisions. The interface relationship also allows for steps to occur simultaneously.

Because it would make the diagram too cumbersome to draw every relationship among steps, we have chosen to show only explicit key decision points and interfaces with lines between the boxes. However, in the discussion of the steps, we point out some of the implicit interactions not shown on the diagram.

We do not intend this to be an all-inclusive framework. Organizations should adapt the framework as appropriate. For example, some organizations do not have the resources or are not required to comply with some of the requirements. While this framework provides some structure for planning, each organization should tailor the framework for its own circumstances.

The WEA Integration Strategy Framework for AOs is shown in Figure 27.

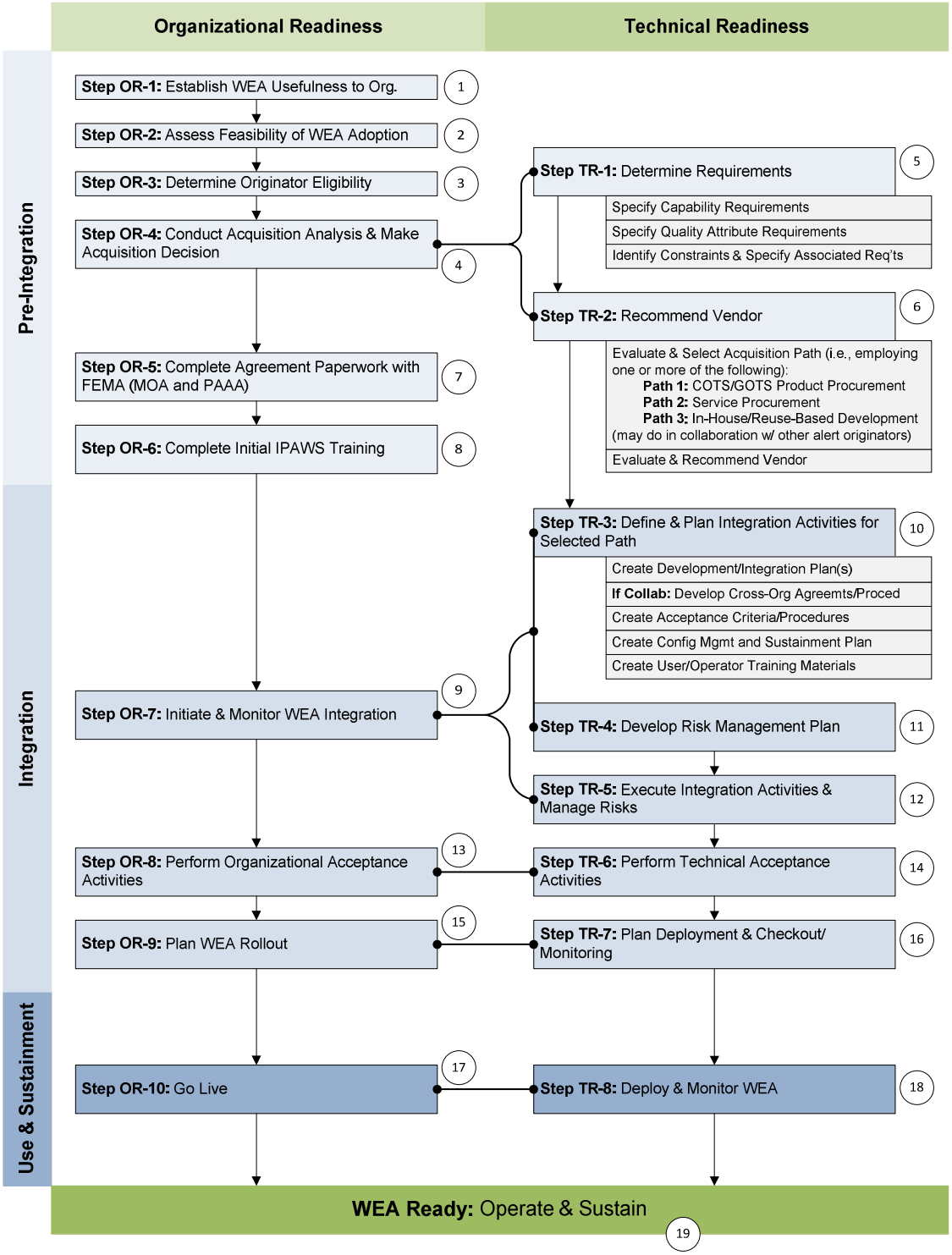


Figure 27: WEA Integration Strategy Framework for AOs

The framework outlines a number of interrelated activities that will enable AOs to achieve the levels of organizational and technical readiness necessary for full WEA adoption and operation.

This framework considers the integration of WEA into an organization's existing emergency-response infrastructure from two interrelated perspectives:

- organizational perspective
- technical perspective

The left side of the diagram contains activities that represent the organizational perspective (shown as steps). Generally, these organizational steps are managerial and oversight activities. In the diagram, Organizational Readiness is abbreviated OR, and each activity has a step number (e.g., OR-1). The right side of the diagram contains activities that represent technical activities. Technical Readiness is abbreviated TR, and each activity has a step number (e.g., TR-1). The technical steps are the responsibility of technical staff directly engaged in the acquisition, development, and deployment of information technology capabilities. However, ORs and TRs may be performed by the same set of individuals. In addition, ORs and TRs have many touch points or interfaces, which the diagram shows as connecting lines with circular end points.

The diagram also contains three vertical blocks on the left side that map to the following phases:

- The Pre-integration Phase contains the activities that happen before an organization begins integration.
- The Integration Phase describes integration activities.
- The Use and Sustainment Phase describes activities to support an achieved and ongoing state of readiness.

Description of Framework Process Steps

Pre-integration Phase

In this section, the organization enters the Pre-integration Phase. We will begin the narrative with Step OR-1: Establish WEA Usefulness to Organization.

① OR-1: Establish WEA Usefulness to Organization

In this step, organizations reason about the usefulness of WEA to them. Questions that organizations may address in this step include

- Do we want to adopt WEA?
- What will it provide for us?
- How will it support our mission and our structure?

This step complements Step OR-2, which addresses the feasibility of WEA adoption. As organizations reason about the business case for adopting WEA, they are likely to consider budget constraints and eligibility requirements, which fall under the purview of OR-2. The exit criteria for this step are that the organization has decided to adopt WEA and needs to begin reasoning about the feasibility of doing so within its context.

② OR-2: Assess Feasibility of WEA Adoption

In this step, organizations assess whether WEA adoption is feasible for them (within their current state of readiness) before they formally apply for eligibility in Step OR-3. Organizations may address questions such as

- Do we have funding for it?
- Do we have the technical capability to build or acquire a system that can integrate with WEA?
- Do we have resources and guidance to train people?
- Do we have operators available and qualified to use WEA?
- Will our organization be eligible (capable of meeting state and federal requirements)?

The feasibility assessment in Step OR-2 may be informal and remain internal to the organization. The exit criteria for this step may include organizational sponsorship for adoption and budget approval to begin the WEA adoption process.

OR-2 also informs Steps TR-1: Determine Requirements and TR-2: Recommend Vendor. We address these technical steps later in the process description; however, in Step TR-2 AOs will specify what software they will use and the path they will use to obtain it (e.g., build it themselves vs. acquire it). So an organization should consider Step TR-2 before moving on to Step OR-3: Determine Originator Eligibility. As mentioned earlier, it would make the diagram too cumbersome to draw every relationship, so we show only explicit key decision points and interfaces. This is an example of the implicit interplay between the organizational and technical considerations.

(3) OR-3: Determine Originator Eligibility

Organizations must determine whether they are eligible to become WEA message originators. Eligibility compliance may be required at both the state and federal levels. FEMA is responsible for dictating the WEA compliance requirements at the federal level. FEMA has more information on eligibility requirements online [FEMA 2013a]. Once organizations have verified that they meet the eligibility requirements, they can start acquisition analysis in Step OR-4. This step is important because organizations should minimize the effort and expense they expend before determining eligibility so they don't waste resources if they can't meet the criteria.

(4) OR-4: Conduct Acquisition Analysis and Make Acquisition Decision

This step starts the acquisition analysis and acquisition decision making. Organizations should follow available acquisition standards and best practices, such as those described in *CMMI® for Acquisition, Version 1.3* [CMMI 2010], to support this step. Relevant best practices include those for acquiring, buying, or building software. Organizations should tailor any best-practices guidance to WEA requirements. This step also kicks off two technical steps, TR-1 and TR-2. We cover these technical steps in more detail next. Generally, they include activities such as drafting requirements, assessing the organization's own technical capabilities, and assessing the capabilities of candidate suppliers.

(5) TR-1: Determine Requirements

Step TR-1 involves determining the requirements for selecting a potential alert-origination system. An organization needs this information to include in acquisition and planning documents, such as an RFP. At a minimum, requirements for WEA-compliant solutions should include a description of the priority

- functional requirements

- quality attribute requirements (e.g., performance, security, availability)
- constraints (e.g., a requirement to integrate with existing emergency-response systems)
- non-technical requirements (e.g., customer support, licensing considerations)

6 TR-2: Recommend Vendor

By Step TR-2, an organization should have some recommendation from the technical staff for an alert-authoring capability supplier (this could be an in-house supplier). The goal of Step TR-2 is to evaluate options and make a final decision on an acquisition path. For example, possible acquisition paths might include

- buy software
- subscribe to service
- share a warning center
- build in-house
- leverage open source

While the decision to acquire or build the capability is ultimately an organizational decision, the organizational and technical staff should work together to make these decisions (as indicated on the diagram by the interface relationship shown between TR-2 and OR-4). In this step, an organization should evaluate design and acquisition strategy tradeoffs as well as cost implications. If the organization decides to procure the system, the technical staff should be involved in evaluating suppliers and should recommend a vendor.

While Steps TR-1 and TR-2 are underway, the organizational staff should start to become familiar with the agreement paperwork in preparation for OR-5.

7 OR-5: Complete Agreement Paperwork with FEMA

In this step, the candidate AO organization completes the agreement paperwork with FEMA such as the MOA and the Application for IPAWS Public Alerting Authority [FEMA 2013a]. Because there are many sub-steps involved in these processes, it may be helpful to request guidance from FEMA or the alert-authoring capability supplier on how to complete the paperwork as efficiently and accurately as possible. For example, the MOA application contains a section that requires the organization to describe the type of alert-authoring software, including the vendor that the organization intends to use. The approval process may be faster if the alert-authoring capability supplier has already signed an MOA with FEMA and successfully integrated its system with IPAWS.

8 OR-6: Complete Initial IPAWS Training

For training, FEMA's Emergency Management Institute offers the independent study course "IS-247.A Integrated Public Alert and Warning System." This course is a prerequisite for full access to IPAWS-OPEN for the purpose of public alerting. Generally, each alert-originating organization must have one certified person to participate. The originator is responsible for planning and executing the organization's own training program. FEMA does not provide training on third-party authoring software [FEMA 2012a]. In addition to required training, some organizations may have optional training for vendor products. For this reason, we named this step "Initial Training." This step also includes a definition of training requirements and ongoing assessment of training gaps

and needs. Organizations may also encourage AO staff to attend relevant conferences to keep skills current and learn from others.

Summary of the Pre-integration Phase. At the end of the Pre-integration Phase, after executing the Organizational Readiness activities, the organization has decided to adopt WEA, completed the paperwork with FEMA, and participated in the initial IPAWs training. After executing the Technical Readiness activities, the organization has identified the acquisition path, selected the alert-authoring capability supplier, and developed the RFP requirements. Both the organizational and the technical activities informed the RFP development in OR-4 and contributed to the evaluation criteria and the technical requirements. The implementation of WEA can now move forward to the Integration Phase.

Integration Phase

9 OR-7: Initiate and Monitor WEA Integration

The Integration Phase starts with the organizational staff in Step OR-7: Initiate and Monitor WEA Integration activities. The monitoring activity is necessary whether an organization is doing in-house development, leveraging a service, sharing capability with another organization, or buying a product. During this step, management is responsible for oversight of the alert-authoring capability supplier as well as the organization's own technical staff. At this stage, the technical staff should begin to plan integration activities and concurrently develop a risk-management plan. The overseeing organization should fund WEA-related activities as required, as well as oversee technical task execution and risk-management processes. Therefore, this step interfaces with technical activities TR-3, TR-4, and TR-5.

In addition to being an acquisition-oversight activity, OR-7 is also an internal activity. Organizations should begin producing their own acceptance criteria and their own sustainment and resiliency plans.

10 TR-3: Define and Plan Integration Activities for Selected Path

This step involves defining and planning integration activities. At this stage, the technical staff should create a development plan based on the acquisition path selected. Depending on the acquisition path, the plan may define activities such as those necessary to develop a new system or integrate with an existing system.

If the integration strategy involves sharing WEA message-origination capability with another organization that already has the capability, the technical and organizational staff may need to work together to develop cross-organization agreement procedures. Collaborative integration strategies will need to cover how the parties will access the capability, service-level agreements, and funding strategy.

The sub-boxes in this step describe some plans and materials that the organization may develop during TR-3. The organization may develop acceptance criteria and procedures at this stage. It will use this information in Step TR-6 to perform acceptance activities. It may develop configuration-management and sustainment plans. These will address questions such as how the organizations will handle upgrades or how the organization will sustain the system over the long term. The

organization may also need to create user (operator) training materials if the alert-authoring capability supplier does not supply them.

Note that the straight-line interface shown between TR-3 and TR-4 indicates that an organization may perform these activities concurrently.

(11) TR-4: Develop Risk-Management Plan

There are business and technical risks associated with WEA adoption, and new risks are likely to arise over time. The organization should continuously manage and mitigate these risks. Therefore, developing a risk-management plan is crucial. This should be done in close collaboration with TR-3: Define and Plan Integration Activities for Selected Path, as indicated by the interface relationship between them. It may be helpful to seek guidance or examples of risk-management plans in cases where organizations do not have them.

(12) TR-5: Execute Integration Activities and Manage Risks

In Step TR-5: Execute Integration Activities and Manage Risks, technical staff executes the integration activities and manages the risk plans developed in Steps TR-3 and TR-4. This step connects to OR-7, which provides organizational monitoring of the technical task execution. The technical execution steps will vary depending on the technical solution and acquisition strategy selected.

(13) OR-8: Perform Organizational Acceptance Activities

An organization should perform acceptance activities from both an organizational standpoint and a technical standpoint. In this step, it is necessary to perform some organizationally focused acceptance activities. The organization has to make sure that the selected solution supports its functional needs adequately. The organization also confirms that the solution supports technical requirements to interface with IPAWS. Therefore, organizational and technical acceptance activities occur concurrently and collaboratively.

(14) TR-6: Perform Technical Acceptance Activities

The organization will assess the technical implementation against the requirements previously defined in Step TR-1. This includes evaluation of functional and quality attribute requirements (e.g., performance, security). This step also involves executing the acceptance procedures developed in TR-3. These acceptance activities should include stress and off-nominal evaluation. Once the technical assessment is satisfactorily completed, the organization should run additional operationally focused activities. The acceptance activity steps may include interaction with vendors and FEMA to ensure that the organization has fully evaluated the capability from end to end.

(15) TR-9: Plan WEA Rollout

Planning the WEA rollout raises a variety of questions:

- Are organizational and technical acceptance activities satisfactorily completed?
- Are deployment plans ready?
- Who will operate WEA for the organization?

- Are they trained?
- How will WEA affect existing processes?
- Is the public ready to receive WEA messages? Are people informed about WEA, and can they interpret 90-character messages?
- Is public response to such alerts sufficiently understood?

Therefore, for members of the organizational staff, part of planning the WEA rollout should focus on public relations. They have to get the word out that this capability will be available to people and prepare materials to explain it to them.

Planning for WEA may also include assessing the readiness of the mobile service providers in the area where the organization will use WEA. For example, organizations could be in an area where some carriers do not support messages formatted in the CAP or have not yet fully integrated with IPAWS. As a result, only part of the community may get a WEA message. An organization should understand these risks and plan for them before deploying WEA.

Much of the technical rollout planning that supports this step occurs in TR-3.

16 TR-7: Plan Deployment and Checkout/Monitoring

In this step, the technical staff will create a deployment plan for WEA and conduct a final pre-deployment check of the system. The pre-deployment check may include activities to verify that WEA is working properly from end to end. The organization will also develop plans for continuous monitoring of system health in this step. Note that deployment is not just a technical activity. The nature of the capability is that it should reach a wide variety of people during a critical time such as during an emergency. An organization should plan for technical deployment from a system-of-systems perspective.

Summary of the Integration Phase. At the end of the Integration Phase, the organization has defined and planned the integration activities for the selected acquisition path and has executed the integration activities up to the point that the WEA capability has successfully met the defined acceptance criteria. The organization also has plans in place for risk management and WEA rollout and sustainment.

Use and Sustainment Phase

17 OR-10: Go Live

In this step, the organizational management gives approval to go live with WEA. The organization will send an announcement about what to expect of the WEA service. This step should not be understood as a one-time event or a simple decision. Going live is basically entering a phase of WEA operation.

18 TR-8: Deploy and Monitor WEA

With approval from the organizational management in OR-10 to deploy WEA, in this step the technical staff executes the deployment and rollout plans defined in Step TR-7. The organization should address several sustainment concerns in this step:

- Will there be scheduled maintenance windows (i.e., times when the system will not be available)?
- Is there a backup capability running elsewhere that the AO can use if the system is down?

In this step, the organization may want to set up monitoring processes to regularly check the health of the system (processes could be manual or automated). Since WEA is used only for limited types of events, the need to use WEA could be as low as once or twice a year. Therefore, to ensure that the capability will be working when AOs need it, continuous monitoring and testing is essential.

19 WEA Ready: Operate and Sustain

The green bar at the bottom of the diagram represents the fact that the organization has achieved readiness (organizationally and technically) and should work on maintaining that state of readiness over the life of WEA operation.

The organizational staff now performs activities such as getting feedback from people and making adjustments in the capability as needed. Organizations may also want to develop WEA guidance materials for their users. The technical staff oversees monitoring mechanisms such as heartbeat (i.e., pinging the system periodically to ensure it is functioning properly). Another health-monitoring tactic is constant checkout, which includes some level of operational testing in addition to pinging the system to make sure it is live.

Of course, the system environment and operational context will continue to change over time. This may affect both organizational and technical activities. For example, staff changes may require training, ID configuration, and other activities. As technical standards evolve, configurations may need to change. In addition, as user needs change, functional and quality attribute requirements such as performance, security, and availability may evolve over time.

Appendix C Mission Thread Workshop

A mission thread describes a set of steps taken to execute a mission. A Mission Thread Workshop (MTW) is a facilitated user-centric exercise to elicit and define operational and identify architecture and engineering challenges and capability gaps for software system solutions. The goal of an MTW is to capture quality attribute and engineering considerations for system-of-systems mission threads from the stakeholders and to identify challenges early in the development life cycle.

The participation of stakeholders is essential to the success of an MTW. These people are typically extremely busy due to their positions in the EMA. To make the best use of their time in the MTW, preparation is critical to providing relevant context and meaningful mission threads that address the capabilities expected of the alert-origination system. To assure that the MTW uses stakeholders' time wisely, we use an engagement approach that consists of three phases:

1. Preparation Phase
2. Conduct Workshop Phase
3. Follow-on Phase

Preparation Phase

In the Preparation Phase, the MTW lead works with an EMA program representative, an architect, and capability subject-matter experts to develop the artifacts needed to support the MTW.

We have numbered the activities performed during the Preparation Phase, but MTW participants will work through many of these steps in parallel.

1. **Review the MTW process.**

The MTW lead provides an overview of the process and examples of two mission threads (one operational and one security focused) with supporting context diagrams. The MTW lead works with the EMA representatives to create a timeline that identifies target dates for developing key artifacts that the MTW lead will provide to the stakeholders before the workshop.

2. **Develop EMA mission and business drivers.**

The EMA program-management representative develops the driver information and provides it to the MTW lead for review and feedback. Based on the feedback, the EMA representatives will update the driver information and create a briefing (e.g., two or three slides) to present it during the workshop. The presentation will give MTW participants an overview of the purpose of the alert-notification operation and the important business drivers and quality attributes that will shape its architecture.

3. **Develop architecture plans.**

The EMA architect develops the architecture plan with feedback given by the MTW team. The EMA architect will then create a briefing to use at the workshop. This presentation will share with the MTW participants the technical considerations, constraints, and drivers that affect the devel-

opment of the architecture used in the alert-notification operation. The information will focus on the vignette and mission thread capabilities.

4. **Develop vignettes, mission threads, and appropriate quality attributes.**

The MTW team meets with the EMA architect and subject-matter experts to do the following:

- Determine the vignettes and mission threads to address in the MTW (one operational and one security focused).
- Develop a graphical representation and description of the vignettes. The graphical representation should show the infrastructure and organizations involved and their relationships (a context diagram).
- Develop the mission thread steps.
- Identify the relevant quality attributes, such as performance, availability, security, scalability, and usability.

These will be the primary inputs to the next phase of the MTW, where stakeholders will augment them to the degree necessary to uncover architectural challenges.

5. **Identify participating stakeholders.**

It is important to identify key stakeholder roles whose participation is essential to the workshop. Examples of stakeholders whom we often seek to involve in an MTW include

- two or three first responders (police, fire, call center operators)
- emergency-operations center operator
- city representative
- state government representative
- alerting-system vendor representative
- member of IT staff
- public-relations representative
- NWS representative

6. **Select the MTW team.**

The MTW team consists of three or more people who perform the four roles of lead, facilitator, scribe, and analyst.

- MTW lead: The lead plans and executes the MTW; he or she may also take one of the other roles during the workshop.
- MTW facilitator: This person facilitates the discussion during the workshop.
- MTW scribe: The scribe documents the discussions that occur during the workshop.
- MTW analyst: One or more analysts listen to the discussion and interject to address quality attribute or engineering considerations that participants do not address.

7. **Settle on logistics.**

Where and when will the MTW be held? Will only on-site stakeholders participate, or does the facility have a network or telecom to support remote personnel? The MTW team and EMA representative will work out these and other necessary details during the Preparation Phase.

The Preparation Phase is carried out via informal interactions between the MTW lead and the EMA representative. They can handle these interactions by whatever combination of telephone, email, and face-to-face communication the parties find most effective and convenient.

At the completion of the Preparation Phase, the MTW team and EMA leads have produced the following outputs:

- one or more vignettes, with an operational and a security mission thread
- mission and business driver presentation
- architecture plan presentation
- list of invited stakeholders and their role and availability for the MTW
- MTW invitation letter
- selection of MTW team
- finalized workshop logistics
- package of MTW preparation material for MTW stakeholders

Conduct Workshop Phase

The focus of an MTW involves augmenting the mission threads with engineering and quality attribute considerations and identifying challenges based on stakeholder inputs and the dialogue between the stakeholders and architects. The workshop will occur over one day. During each step, the facilitator guides the discussion, and the scribe documents the quality attribute augmentations and any issues that arise for each mission thread.

1. **Present the MTW.**

In this step, the MTW facilitator describes the MTW technique to the assembled stakeholders. The presentation should take 5 to 10 minutes and will include

- the MTW steps briefly
- the use of vignettes and mission threads to elicit stakeholders' participation in the discussions
- the MTW team and their roles during the MTW
- the outputs from the MTW (augmented mission threads and challenges)

The facilitator will also use this time to explain the technique, provide the stakeholders with an opportunity to ask questions about the technique, lay the ground rules, and set expectations for the workshop. The facilitator also informs the stakeholders that the MTW team will strongly facilitate and document the workshop so that they can focus on the discussion.

2. **Present the business and mission drivers.**

An EMA program representative presents the business and mission drivers, including the business and programmatic context; high-level functional requirements, constraints, and quality attribute requirements; and the plan for development. During the presentation, the facilitator gives the stakeholders and the MTW team opportunities to ask questions related to the business and mission

drivers. The presentation could take up to 30 minutes, depending on the number of questions that arise, but the facilitator should ensure that it does not exceed this time frame.

3. **Present the architectural plan.**

The EMA architect presents the architecture-development plans, including key business and programmatic requirements, key technical requirements and constraints that will drive architectural decisions, existing context diagrams, high-level diagrams and descriptions, quality attributes, development spirals, and the integration schedule. The goal of this presentation is to provide the architect's vision. Stakeholders and the MTW team can ask questions dealing with the development plan. The presentation could take up to 30 minutes, but the facilitator should ensure that it does not exceed this time frame.

4. **Review the vignette.**

The EMA architect or a representative presents the vignette and the first mission thread that participants will augment in the MTW. The vignette provides the context for the mission thread. It should help the stakeholders understand the environment in which the mission thread steps will occur. Reviewing the vignette typically takes 5 to 10 minutes, and all participants have an opportunity to ask questions about the vignette and context diagram.

Due to the scale of the alerting infrastructure involved, the MTW participants should narrow the vignette's context information with a set of assumptions that focus on the environment in which the mission will take place.

The MTW facilitator will redirect detailed questions about the mission thread assumptions, steps, and possible extensions to Step 5.

5. **Augment the mission thread.**

The MTW facilitator proceeds to describe the mission thread by starting with the assumptions listed in the mission thread. The facilitator asks the stakeholders if they have any questions, additions, or clarifications to the assumptions listed in the mission thread. The facilitator should allow 5 to 10 minutes to discuss, understand, and clarify the assumptions but not much longer because as participants consider each step, they will identify additional assumptions for the scribe to document. The facilitator next leads a short discussion that addresses the nodes and actors for this mission thread, for understanding and clarification.

The facilitator then proceeds to discuss each step with the stakeholders until they have covered all the steps in the mission thread. The goal is to spend about two hours on each mission thread while performing Steps 5 through 7, but typically the first mission thread will take longer while the stakeholders learn the technique.

The MTW facilitator leads discussions of each step to elicit and clarify requirements; identify possible architectural and engineering challenges, new use cases, and capability gaps; and reason about applicable quality attributes that participants have identified. Stakeholders are encouraged to ask questions and raise issues for each step, while the facilitator keeps the discussions on track and in scope. An MTW scribe captures the relevant points from the discussions for each step and documents them in the MTW template.

6. **Consider extensions to the mission thread.**

During the stakeholder discussion, the group may decide that a mission thread step needs extensions to enable future analysis of different aspects of the thread. The focus during the workshop is on discussing each step and not on spending a lot of time considering alternative paths. Typically, we have found that these extensions address system use cases that workshop participants had not previously considered but that should be investigated. The scribe documents the extensions, and the facilitator returns the discussion to the mission thread steps.

7. **Discuss overarching quality attribute considerations.**

Once workshop participants have considered all the steps of the mission thread, the MTW facilitator encourages stakeholders to discuss each identified key quality attribute from the perspective of the entire mission thread. Up to this point, quality attributes have been considered at the step level, but it is also important to consider the key quality attributes of the mission thread from end to end. The MTW facilitator ensures that stakeholders discuss each overarching quality attribute and that the MTW scribe captures all issues and concerns in the MTW template. The MTW facilitator elicits discussion from the stakeholders until they have covered the entire set of quality attributes. Sometimes the group will capture a consideration that relates to a specific step in the mission thread; it is fine to go back and update that thread augmentation at this time.

8. **Analyze remaining mission threads.**

The MTW facilitator will repeat Steps 4–7 for the remaining mission threads to be covered in the workshop. If major issues and challenges arise that were previously captured in the MTW, the scribe can reference them at the step in which they emerge in the mission thread while the participants choose to discuss only new considerations on that issue in further detail, in order to use the stakeholders' time effectively.

Follow-on Phase

The first task for the Follow-on Phase is to "scrub" the augmented mission threads. The information that the scribe documents during the Conduct Workshop Phase is raw information. After the workshop, the scribe will expand that raw information into sentences and phrases that make sense and reflect the information discussed. The scribe's role is a challenging one because he or she must listen to the discussion and document it while the discussion continues. After revising the comments section in the template, the scribe will reference each comment by a unique identifier. This will help the MTW team identify and document the architectural, engineering, and capability challenges.

Once the MTW team members have completed these activities, they will organize the assumptions from the thread, the engineering considerations from each thread step, and the quality attributes for each thread into a group of challenges. The MTW team documents each challenge by listing its source(s) in a table that maps challenges to contributing steps of the augmented mission thread. To produce the list of challenges, the MTW team

- reviews the steps one by one and forms a list of challenges, noting which steps contribute to which challenges in a cross-referencing table
- reviews the relevant quality attributes and inserts any additional challenges

- reviews the challenges and combines similar challenges to reduce the number (typically to about five to seven), changing the cross-references to the contributing steps accordingly

The MTW team will then distill the challenges into a short report for the stakeholders. This summary report will include the table of combined challenges, the description of each challenge, the impact of each challenge on mission and business goals, and a set of recommendations for resolving the challenge. The MTW team reviews the report with the EMA leadership and makes appropriate changes to clarify the issues and correct any misunderstandings of the MTW team. The MTW team then delivers a final presentation to stakeholders. The team should complete the Follow-on Phase within a few weeks after the workshop.

Appendix D Mission Thread Workshop Results

This appendix provides an example mission thread and results from MTWs conducted with the Harris County Office of Homeland Security and Emergency Management (HCOHSEM), Houston, Texas, and the Jefferson County Emergency Communications Authority (JCECA), Lakewood, Colorado.

Describing an Operational Mission Thread

Table 10 shows an example of the first 10 steps of an emergency scenario used in the Harris County and Jefferson County MTWs. Each workshop used an operational mission thread that described a hazardous-material accident in a residential area. Discussions during the workshop clarified the actual operational environment.

Table 10: Hazardous Material Accident Mission Thread for Emergency Management

Mission Step	Time	Description (Fill in Prior to MTW)
1	May 17, 2012, 1:30 pm	A large truck carrying pesticide approaches a traffic light at the intersection of XXX and YYY. The traffic light has already turned "YELLOW."
2	1:31 pm	The truck proceeds through the traffic light even though the light has turned "RED."
3	1:31 pm	An SUV driving on YYY hits the truck broadside as both cross the intersection. Both vehicles burst into flames, which causes traffic to be blocked in all directions.
4	1:32 pm	Several civilians in cars that were approaching the intersection call 911 to report the accident. Other civilians rush to assist the accident victims.
4a	1:33 pm	Dispatch center sends first responders. Ten minutes or less response time outside city limits; five minutes or less in city limits.
5	1:34 pm	The driver of the SUV is pulled from the vehicle and placed in the front yard of a home upwind of the smoke from the fires. The driver of the truck was killed in the accident. The smoke starts to drift toward a residential area and an elementary school.
6	1:37 pm	Police usually arrive first and take control in the following areas: 1. Secure the scene 2. Change traffic patterns 3. Keep crowd away Fire department will probably arrive shortly after police and perform a 360 degree "size-up" to determine whether they can handle with their on-site resources.
7	1:39 pm	Several bystanders near the smoke complain of burning eyes and lungs.
8	1:52 pm	Firefighters are able to deploy at the accident and start to extinguish the fire. Will establish a unified command at this point (a work in progress). Updates will be sent to the emergency operations center (EOC). Harris County hazmat average response time is 20 minutes within city.
9	1:55 pm	The pesticide truck explodes, which results in fatalities (14 people: 6 firefighters, 3 police officers, and 5 civilians) and injuries (10 people: 1 firefighter, 2 EMS, and 7 civilians), and ignites seven car fires close to the explosion.
10	1:57 pm	A radio report of the explosion has started to draw the parents of the children in the elementary school as well as other bystanders to the area. This adds to the overcrowded road situation and results in several vehicle accidents, which start to interfere with additional emergency vehicles' access to the site.

Eliciting Drivers from MTW Discussions for WEA Implementation

During each workshop, facilitators gathered additional information on each step of the mission thread. This additional information elaborated on the operational challenges that are associated

with the mission steps and drivers for decision making. Then the MTW team identified operational challenges from this information. Table 11 lists some examples of elaborations related to Step 9 of the mission thread.

Table 11: Mission Thread Step 9 and Elaboration

Mission Step	Time	Description (*Fill in prior to MTW)*	Elaborated Information from Workshops with HCOHSEM and JCECA
9	1:55 pm	The pesticide truck explodes, which results in fatalities (14 people: 6 firefighters, 3 police officers, and 5 civilians) and injuries (10 people: 1 firefighter, 2 EMS, and 7 civilians), and ignites 7 car fires close to the explosion.	9-1 The response plan needs to be reviewed to assess what happens when fatalities occur. 9-2 Incident paralysis. Responders will withdraw to safety. Taught to expect another explosion. Survivors will call dispatch center to report situation and ask for additional resources. 9-3 EOC will get a phone call from someone. Depends on who got killed during explosion. EOC is also likely to have been monitoring the situation. *Shelter in place or evacuation order*, then EOC expects phone call (not email or text). The EOC expects that the ground truth is not really known at this point. EOC starts engaging with the "internal message" to officials and partners; nothing pushed up to the JIC (Joint Information Center) at this point. Will push out broad information that something bad is happening. Going from Level 4 (normal) to Level 3 (increased readiness) (Levels of readiness are covered in the plan in some detail. Level 1 would involve long-term recovery; Level 2 would be extended days of operation.) Industrial liaison would likely relocate to the EOC. Within 15–45 minutes, the EOC room might be activated. 9-4 The organizations have continuity of operations and succession plans to keep things going in the face of personnel changes. 9-5 EOC has access to media feed. Can coordinate with an incident of this severity. The media have been good about helping with hazmat situational awareness. Can get downlink in some of the responder vehicles. This has proven to be an important surveillance tool. 9-6 Call for backup. Media will swoop in. Major, major response. Three more alarms of fire equipment will likely be dispatched. 9-7 State will be notified. The state will probably have already called the duty officer. Start of a dialogue. When things get sufficiently bad, someone from state would physically relocate to Harris EOC. Notification to FEMA might happen at this point. 9-8 Might have a call out to alert for hospital needs. A big part of the response would be to treat burn victims. Medical examiner's office. Texas Medical Center involved. 9-9 Once a person from OEM or Fire Marshall Office on scene, that is considered trusted agent conveying accurate information back to EOC. 9-10 NWS will be monitoring the situation and taking action as needed. Can support with feed. 9-11 Assumption modification: Assume WEA is up and running. Would work with incident command to figure out what information should go out. Check with incident commander to ask what the public information needs are. *Shelter in place* with threat to life would reach a threshold. Prioritize the life/safety messages; see if already covered by template messages; draft the message; get approval by incident command; evaluate whether the message will accomplish what needs to happen. Understand that if a WEA message needs to go out, it needs to go out quickly.

Analyzing Drivers to Identify Challenges and Recommendations

MTW teams analyzed the information obtained during the workshops with HCOHSEM and JCECA to determine categories of challenges and recommendations for WEA implementation. Results from each workshop describe these challenges and a set of recommendations for each organization. The challenges and recommendations in this section are reprinted or adapted from the complete workshop reports from HCOHSEM and JCECA.

Harris County Office of Homeland Security and Emergency Management (HCOHSEM)

Challenge 1: Acquiring the resources (funding and staffing) to integrate and sustain a unique WEA messaging capability into their operations

> *Recommendation:* Explore obtaining funding or product licenses from DHS and/or FEMA that provide the WEA messaging capability, as DHS and FEMA have done with some previous emergency alerting systems.

Challenge 2: Setting up a collaboration between resource-rich agencies and resource-poor agencies to provide WEA messaging capability

> *Recommendations:*
>
> - Provide governance and communication support at the state level to facilitate the dialogue between potential collaborating agencies.
> - Study the possibility of teaming with the local NWS offices to see if they could incorporate civil emergency-alert messages in the current or future versions of NWS's system, which provides WEA messages.

Challenge 3: Sharing mature situational-awareness capability with first responders and other key partners

> *Recommendation:* Host information sessions with the first responder and partner communities to identify what current situational applications they have or are planning to implement at the HCOHSEM Operations Center. Based on the feedback, consider whether it would make sense to work toward providing these capabilities to the communities.

Challenge 4: Defining criteria for determining when to send a WEA message

> *Recommendations:*
>
> - Identify and develop civil emergency scenarios that HCOHSEM can discuss with the first responders and partner communities to determine a consistent approach for issuing WEA messages.
> - Host meetings with NWS, FEMA, DHS, and the state of Texas to share information about when it is appropriate to send a WEA message.

Challenge 5: Ensuring that alerting products will meet operational and sustainment needs now and into the future

Recommendations:

- Hold periodic meetings with the EAS vendor that provides WEA messaging capability to discuss feedback and lessons learned from using their product and to learn what new features are in development.
- Hold periodic meetings with the CMSPs that cover HCOHSEM's area of interest to understand their current and planned WEA messaging capabilities and coverage. Monitor the CMSPs and the geotargeting capabilities (FIPS code, polygon, or circle) that they use to support WEA messaging to help understand the effectiveness of alerts issued.

Challenge 6: Handling of information generated and used within alerting operations from a security perspective appropriate to support HCOHSEM's mission and goals

Recommendations:

- Study the security of information used and generated within alert operations.
- Hold periodic meetings with the vendor that provides WEA messaging capability to share HCOHSEM's security concerns and issues and to learn about the vendor's secure coding practices and security approach for the product.
- Plan for future increases in use of video information from cell phones, law enforcement cameras, and the news media during civil emergencies and its implications for the computer infrastructure as well as security of the video data.

Challenge 7: Mitigating the lack of infrastructure support for the anticipated volume of requests for additional information via phone, email, and website channels in response to issuing a WEA message

Recommendations:

- Consider a study to assess the EMA's ability to support the volume of information requests anticipated when issuing a WEA message.
- Consider holding meetings with other EMAs that have implemented mass-notification systems to get a feel for the volume of requests for information they receive after sending out an alert message. With this information, scale the information to reflect the number of citizens that HCOHSEM supports.
- Consider developing public-awareness training for the citizens served by HCOHSEM to help them understand what a WEA message represents and its content.

Jefferson County Emergency Communications Authority (JCECA)

Challenge 1: Developing criteria for an emergency that warrants issuance of a WEA message

Recommendations:

- Use the Hazardous Material Accident mission thread (see Table 10) as a starting point and create additional mission threads that reflect emergencies that JCECA can use to analyze and assess what alert methods would be appropriate and when JCECA would use them to alert county citizens.

- Collaborate with neighboring EMA jurisdictions and the state to develop consistency in how to handle alerts and when to communicate the information to the public via different channels. Use the mission thread approach to do this.
- Use the additional mission threads and collaboration results to develop a list of actions, prioritize those actions, and then determine the threshold for issuing a WEA message.
- Establish an emergency-management plan that clearly documents all the information and agreements and describes the process for determining if a particular event warrants a WEA message, possibly through the use of a flow diagram.

Challenge 2: Handling the volume of 911 calls during an emergency while providing timely notification to the public

Recommendations:

- Develop information to help the public understand how a 911 call is received and handled and where to find additional information during an emergency.
- Re-examine how 911 calls are handled; consider, for example, providing a message that states the current information about an incident after the Public Safety Answering Point (PSAP) receives more than a certain number of calls.
- Perform a study to understand the actions involved when 911 calls are rolled over to other PSAPs when a PSAP becomes overwhelmed.
- Consider developing operational procedures that deal with the rollover of 911 calls and how to provide consistent information to the public.

Challenge 3: Handling current and additional inputs (911 text messages, video inputs, etc.) to develop situational awareness of an emergency and to support when it is appropriate to set up an EMA

Recommendations:

- Augment the mission threads developed in the recommendations for Challenge 1 to reflect the envisioned information inputs; then use the process with stakeholders to discuss the potential impacts and create strategies to address.
- Use these results to consider the system upgrades planned for the near future. Perform a study of when to use WebEOC in developing the situational awareness of an emergency and in setting up an EMA, with the idea of possibly having a better picture for applying resources.

Challenge 4: Incorporating cybersecurity into JCECA's operational and support operations

Recommendations:

- Study the security of information that JCECA uses and generates within alert operations.
- Research best practices identified for cybersecurity to see what practices would be most helpful for JCECA. Begin by checking the following websites:
  - http://www.dhs.gov/topic/cybersecurity
  - http://www.cert.org/

  - http://cve.mitre.org/
  - http://www.microsoft.com/government/en-us/guides/pages/cybersecurity.aspx
- Consider meeting with vendors of the emergency notification system (CodeRED) and incident management (WebEOC) on a periodic basis to understand their security practices in developing and maintaining the applications.

Challenge 5: Coordinating procedures, training, and communication within JCECA, as well as with neighboring EMAs and the state

Recommendations:

- Develop operator procedures that support the alert-severity levels defined in Challenge 4 and provide the associated information to the public in the time frames prescribed.
- Consider having all PSAP operators trained to handle both police and fire incidents.
- Hold periodic meetings with neighboring EMAs and the state to improve coordination efforts between the groups, taking advantage of the information and material that JCECA has and is developing.

Appendix E Using a Hazardous Materials Mission Thread to Define Testing Considerations

In Section 9, we discussed three testing chains and illustrated them in Figure 16. The easiest way to obtain data for these tests is to create scenarios that define specific situations, and one way to do that is to use mission threads such as described in Appendix C. Figure 28 shows the alerting pipeline beginning with the AO and ending with the mobile devices. Each test chain in Figure 16 begins with the AO and ends at the corresponding numeral.

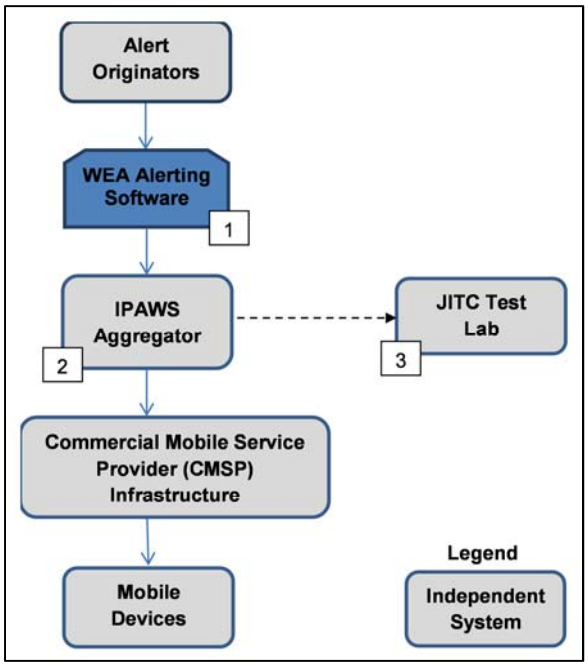


Figure 28: Alerting Pipeline

An EMA obtains the test data by examining the developed mission thread, such as the mission thread in Table 12. The Assumptions and Environmental Context rows provide the preconditions, such as what the emergency is and where it is, that must be set up before a test is run. Then the EMA derives the required data from the steps in the thread. To help clarify the configuration of the system to be tested, the EMA should construct a diagram such as shown in Figure 29. When the EMA executes a test, the test evaluator can trace the path that the execution took through the system on the diagram. A well-tested system will have at least one trace on each connection in the diagram.

To test Chain 1, the AO composes a message appropriate to the test case derived from the mission thread and enters the message in the alerting software. In Figure 29, the AO uses a remotely hosted emergency notification system (ENS) to enter and send the WEA message. There should be indications on the screen, such as an echo of the message text, that allows the originator to determine that the software is operating correctly. Some vendors have built-in verifiers in the origination software that also indicate whether the message, target area, and other parameters are within acceptable limits.

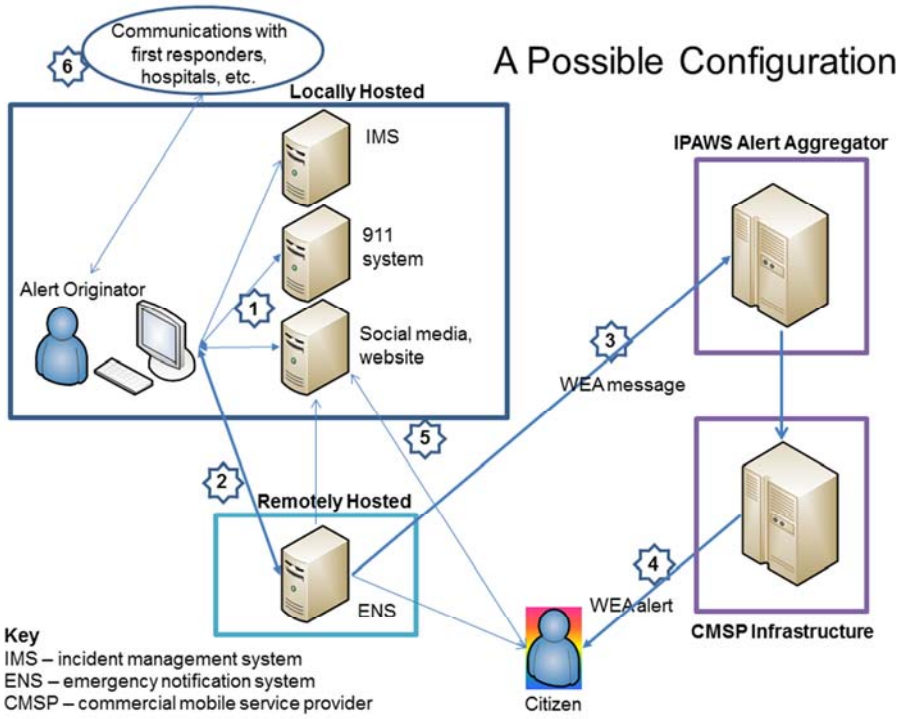


Figure 29: An Elaborated Origination Environment
Note: Starred numbers cross-reference to Table 12.

Chain 2 may be used only by a vendor, but the vendor may be willing to run tests that the EMA requests, particularly if those tests are acceptance tests that are part of an RFP.

To test Chain 3, an authorized EMA may be able to access the JITC test lab. The origination software will have to be reconfigured to send to a different URL. A test case can be entered into the originating software and issued in the usual manner. The instructions for using the JITC test lab will explain how to check the results of issuing the alert. Note that after the message leaves the normal flow, the processing is simulated and may or may not accurately represent actual operation.

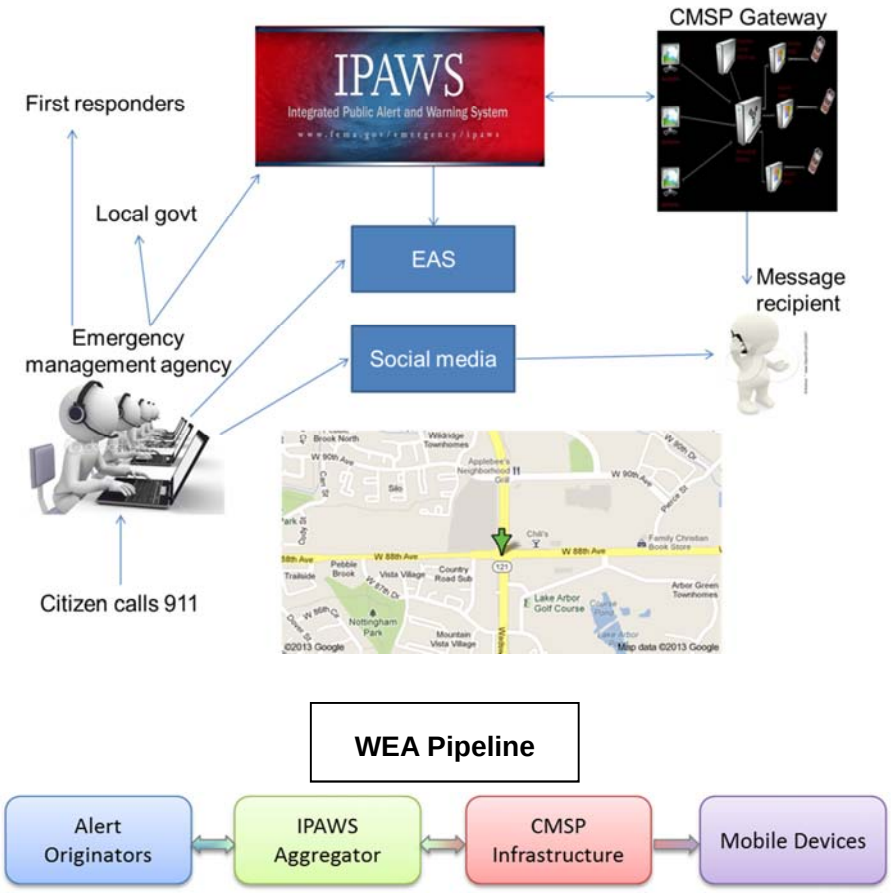
Additional Thread Details

For each mission thread step, Table 12 lists typical activities associated with the step. With this additional information, the EMA should identify which points to consider for testing. The mission thread focuses on the following areas:

- the interface from the operator to the alert-authoring software application
- the application itself
- the interface from the application to the IPAWS Aggregator

Table 12: Example Mission Thread and Steps

Name	Hazardous Material Accident: Truck Explosion with Pesticide and Secondary Explosion
Vignette (Summary Description)	This mission thread highlights the operational tasks and functions associated with a hazardous material accident in a residential area near the borders of Jefferson and Broomfield Counties close to the Denver–Boulder Turnpike. It includes communications and interactions to address the accident, the response, and the alerts sent to citizens based on the accident.

Nodes/Actors	Civilians, police personnel, fire personnel, Jefferson County EOC, PSAPs, middle school, NWS, neighboring county/city EOCs, IPAWS, CMSPs, and cell phone subscribers
Assumptions	Wind is from the northeast at 15 mph. Temperature is in the high 70s. Traffic lights are functioning properly. Jefferson County EOC has been authorized and has the capability to transmit WEA messages. Some but not all neighboring counties can originate CAP and other EAS alerts. All systems used by Jefferson County EOC are available and operational. All WEA service functions are available and operational. WEA pipeline consists of AOs, IPAWS Aggregator, CMSP infrastructure, and mobile devices
Environmental Context Diagram	

Mission Steps	Time	Description *Fill in prior to MTW*	Testing Considerations, Issues, and Challenges	Testing Diagram (Figure 29)
1	May 17, 2013 (Friday), 1:30 pm	A large truck carrying pesticide approaches a traffic light at the intersection of 88th Avenue and Wadsworth Blvd. The traffic light has already turned "YELLOW."	No testing considerations	
2	1:31 pm	The truck proceeds through the traffic light even though the light has turned "RED."	No testing considerations	
3	1:31 pm	An SUV driving on Wadsworth Blvd. hits the truck broadside as both cross the intersection. Both vehicles burst into flames, which causes traffic to be blocked in all directions.	No testing considerations	

Mission Steps	Time	Description *Fill in prior to MTW*	Testing Considerations, Issues, and Challenges	Testing Diagram (Figure 29)
4	1:32 pm	Several civilians in cars that were approaching the intersection call 911 to report the accident. Other civilians rush to assist the accident victims. 1. 911 call center or PSAP begins to receive calls from the public about the accident. 2. (Near-term future consideration) PSAP starts receiving 911 text messages from the public about the accident.	1. Operational procedures for handling 911 calls are based on differing volumes of calls being received. 2. Load testing of 911 call reception capabilities. 3. Is the information being taken related to the 911 calls used in the ENS and/or the incident management system (IMS)? If it is, then how is the information shared? 4. How are the 911 text messages handled?	1 1 2 1
5	1:34 pm	The driver of the SUV is pulled from the vehicle and placed on a lawn on the corner upwind from the smoke from the fires. The driver of the truck was killed in the accident. The smoke starts to drift toward a residential area and a middle school. 1. PSAP dispatcher deploys the police, fire, and EMS units to the accident. 2. (Future consideration) Public provides video of the accident scene.	1. Support/capacity to receive video information.	1
6	1:37 pm	Fire rescue and police arrive on the scene but have difficulty getting close enough due to the blockage of vehicles and bystanders. 1. Dispatcher is in radio communication with the deployed units, which have arrived on scene. 2. A unified command center is set up, and initial assessment of accident is performed. 3. Information about the accident starts to be composed for the public.	1. Communications a. Radios interoperability b. Cell phone 2. How the ENS and/or IMS are accessed by the operators? 3. How is information shared between the ENS and IMS?	2
7	1:39 pm	Several bystanders near the smoke complain of burning eyes and lungs. 1. Hazardous materials (HAZMAT) situation has been identified. 2. Unified command center identifies to dispatcher that additional resources are needed.	No testing considerations	
8	1:52 pm	Firefighters are able to deploy at the accident and start to extinguish the fire. 1. Unified command center continues to provide information to dispatcher.	1. Information starts to be provided to the public via ENS, IMS, a website, and social media.	5
9	1:55 pm	The pesticide truck explodes, which results in fatalities (14 people: 6 firefighters, 3 police officers, and 5 civilians) and injuries (10 people: 1 firefighter, 2 EMS, and 7 civilians) and ignites seven car fires close to the explosion. The blast blows out windows in a 500-foot radius and damag-	No testing considerations	

Mission Steps	Time	Description *Fill in prior to MTW*	Testing Considerations, Issues, and Challenges	Testing Diagram (Figure 29)
		es the water lines below the intersection. 1. Unified command center is affected by explosion and required to redeploy to an area farther from the scene. 2. Increased radio communications between first responders and dispatcher/PSAP. 3. Spike upward in 911 calls to PSAP. 4. (Future consideration) Spike upward in 911 text messages to PSAP.		
10	1:57 pm	A radio report of the explosion has started to draw the parents of the children in the elementary school, as well as other bystanders, to the area. This adds to the overcrowded road situation and results in several vehicle accidents, which interferes with additional emergency vehicles' access to the site. 1. Unified Command Center communicates with hospitals to assess bed and emergency room capacities. 2. Unified Command Center communicates with school district on situation. 3. Unified Command Center communicates with NWS about weather conditions. 4. Increase in calls to PSAP from parents of the school children concerning status of accident and impact on the school.	1. A WEA message is developed and transmitted via ENS or IMS. a. Need to understand how WEA message gets from ENS or IMS to the IPAWS Aggregator. b. Need to understand the security considerations used in the development of the ENS or IMS. 2. Communications with hospitals, school district, NWS, and neighboring jurisdictions and potentially with federal agencies. 3. Need to understand the coverage provided by the CMSPs in the EMA's jurisdiction.	3 2 6 4
11	2:15 pm	Police are able to redirect traffic away from the explosion scene, and emergency vehicles are now able to proceed to the location. 1. Based on information provided, school district decides to evacuate the children from the school. 2. Additional resources are arriving at the scene.	1. Ability to support the requests for information via different channels (telephone, website, social media, etc.).	5
12	2:45 pm	The fires have been extinguished from the original accident, the explosion, and the resulting additional car fires. 1. School evacuation begins. 2. EMS personnel continue to treat the injured and begin their transportation to the hospitals.	No testing considerations	
13	3:15 pm	All injuries and fatalities have been transported from the scene. 1. Organizations involved with the community's infrastructure arrive (power, telephone, water, etc.).	No testing considerations	
14	5:30 pm	Preliminary investigation of the scene has been completed.	No testing considerations	

Mission Steps	Time	Description *Fill in prior to MTW*	Testing Considerations, Issues, and Challenges	Testing Diagram (Figure 29)
15	6:15 pm	All damaged vehicles are removed from the area, and repair crews are able to begin their work.	No testing considerations	
16	May 18, 11:15 pm	Repairs are completed to the street and local infrastructure.	No testing considerations	
17				
18				

For example, if the operator interfaces with the alert-authoring software application via the internet, then the EMA should develop a test procedure that periodically tests the primary and backup methods to log into the application. For the alert-authoring application itself, the EMA needs to talk with the alert-authoring application provider to understand the following:

- how its data centers are architected in terms of hardware and software
- how it performs testing on the data centers
- how it handles upgrades and updates for both hardware and software
- its software-development process
- its security considerations

Gathering this information will help the EMA understand what the vendor is doing and the possible impacts to the system. The EMA should also ask the application vendor about the connection from the application to the IPAWS Aggregator, to understand how the vendor has implemented it and tested it. The application vendor may offer different levels of support related to these last two areas, so EMAs should determine what level of support will meet their needs.

Summary

This appendix describes an approach to developing test cases for WEA messages using an operational mission thread. Each thread should include

- vignette description; nodes, actors, and assumptions; and environmental context
- top-level mission thread (nominal conditions): sequence of steps describing the event and the WEA response
- list of extension steps: mission thread steps representing off-nominal conditions
- overarching quality attribute considerations: considerations and issues not captured in the mission steps

EMAs can derive test cases by establishing a sequence of actions and adding the expected result if the actions happen in the given order.

Appendix F Example Exploratory Requirements

Example Summary

As EMAs consider exploratory scenarios, we suggest they do some creative thinking about how they could leverage an alerting capability during an event with only a few seconds to spare. Here we provide an example of forward-looking requirements that explore the potential for using WEA for a hazardous-spill scenario. In this example, the SEI team collaborated with an emergency-alert expert to develop a set of functional requirements that specifies four types of tiered alerting capabilities. Type 1 is a foundational level and Types II, III, and IV build on Type 1.

To summarize the message tiers in Figure 30,

- Type I uses a computer interface to send an alert.
- Type II uses a computer or mobile handset interface to send an alert.
- Type III sends an alert through the push of a button.
- Type IV will send an alert if conditions meet a certain threshold (e.g., heat, leakage).

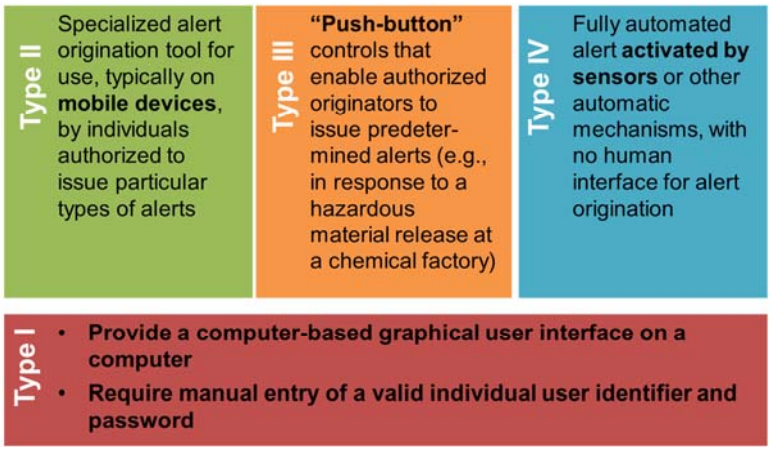


Figure 30: Tiered Functional-Alerting Specifications [Data from interview with Art Botterell]

A variety of channels including sirens, the media, telephones, and IPAWS/WEA may all be notified automatically for Types III and IV. In summary, using scenarios to develop functional requirements can help EMAs come up with creative ways to use powerful resources like WEA.

Example Details

- **Type I:** General alert-origination solution that provides full capability and flexibility to authorized AOs
- **Type II:** Specialized alert-origination solution for use, typically on mobile devices, by individuals authorized to issue particular types of alerts
- **Type III:** Push-button controls that enable authorized originators to issue a small number of predetermined alerts based on specified circumstances (e.g., in response to a hazardous-material release at a chemical factory)

- **Type IV:** Fully automated alert generators operating under the responsibility of an authorized AO and activated by sensors or other automatic mechanisms

A Type I general alert-generation solution shall

- provide a computer-based graphical user interface on computers using Microsoft Windows, Apple, and Linux, and on mobile devices* including at a minimum Apple- and Android-based devices
- require manual entry of a valid individual user identifier and password previously established through the authentication-control interface before performing any operations on or using the solution
- enable authorized AOs to
  - select from alerting zones previously configured on the local control system
  - plot new alerting zones on a map for use in an alert
  - select and edit message templates previously configured through the administrative interface in one or more languages
  - using either templates or entirely original text, compose a CAP alert compliant with, and containing all elements required by, the CAP 1.2 specification* and the FEMA IPAWS Profile for WEA transmission, including all enumerated values for the CAP <category> and <responseType> elements
  - select from previously sent and not-yet-expired alerts and create updates to or cancellations of those alerts
  - review and revise the alert, update, or cancellation prior to release
  - apply a digital signature to the approved message using the FEMA-compliant certificate associated with the AO's identity
  - transmit the approved alert, update, or cancellation to IPAWS and to any local warning systems
- notify the originator promptly if the alert generates an error response from IPAWS or any local warning system
- maintain a complete auditable record of all alerts issued, updated, or cancelled, and of all system confirmations and all errors including authentication failures; maintain such records within the control system for the preceding 12 months; and provide a method for transferring older records to external archival storage prior to their deletion
- enable authenticated administrators to
  - add, edit, and delete authorizations for users
  - manage FEMA-compliant digital certificates associated with individuals
  - add, edit, and delete predetermined alerting-zone definitions, which shall include CAP values such as areaDesc, geocode, and geometry (polygon and/or circle) values
  - add, edit, and delete prewritten, fill-in-the-blank alert templates in multiple languages
  - view and export to archival storage the log of all system activities and errors
  - perform any other configuration or administration functions
- utilize encrypted communications using Transport Layer Security or equivalent link security for all network communications
- allow the AO to select and apply existing test sequences

- notify authenticated administrator of critical system needs such as approaching certification expiration

A Type II specialized alert-origination solution shall conform to the requirements for a Type I solution EXCEPT that

- the user interface may be designed exclusively for mobile devices using, at a minimum, the Apple or/and Android operating systems
- the targeting of alerts MAY be restricted to selection predesignated zones
- the list of selectable values for the CAP <category> and <responseType> elements may be restricted to reflect the responsibilities of the user

A Type III push-button alert-origination solution shall conform to the requirements for a Type II solution EXCEPT that

- the AO interface may be constructed of mechanical push buttons, key switches, or their digital analogues
- user options shall be limited to a small set of predetermined alert templates with automatically updated elements related to time, parameter values (such as current wind conditions), or other details

A Type IV automated alert-origination solution shall conform to the requirements for a Type III solution, EXCEPT that

- there is no human interface for alert origination
- criteria for automated alert origination shall be adjusted through the administrative interface

Appendix G Resources

This appendix provides materials that AOs may consult for more information on the following topics: alert types, alerting authority, the benefits of WEA, developer information, device information, education for public awareness, education on technical topics, geotargeting, standards and tools, strategic plan examples, and WEA real-time use examples.

Alert Types and Information

- ***AMBER Alerts and Wireless Emergency Alerts/Commercial Mobile Alert System –*** Site for the National Center for Missing & Exploited Children; describes WEA approach to AMBER Alerts, one of the three types of alerts sent as a WEA message. http://www.missingkids.com/amber/wea
- ***Mobile weather warnings on the way! –*** NOAA (National Oceanic and Atmospheric Administration, Department of Commerce) site that explains the types of warnings that the National Weather Service will issue and provides general information about WEA messages. http://www.noaa.gov/features/03_protecting/wireless_emergency_alerts.html
- ***Wireless Emergency Alerts (WEA) –*** FCC site that provides answers to general questions about WEA, including what it is, how it works, what it costs (nothing), and other questions. http://www.fcc.gov/guides/wireless-emergency-alerts-wea
- ***Wireless Emergency Alerts (WEA) –*** FEMA question-and-answer site on WEA messages. https://www.fema.gov/wireless-emergency-alerts

Alerting Authority

- ***Alerting Authorities –*** FEMA site with questions and answers on becoming an alerting authority, including steps for signing up for IPAWS. http://www.fema.gov/alerting-authorities
- ***Integrated Public Alert & Warning System Authorities –*** FEMA listing of localities by state that have completed necessary authentication steps to use IPAWS. Within each state category, there are counties and cities listed as well. http://www.fema.gov/alerting-authorities/integrated-public-alert-warning-system-authorities

Benefits

- ***IPAWS Benefits for Alerting Authorities: Integrated Public Alert and Warning System (IPAWS) Fact Sheet –*** FEMA information on the benefits of the internet-based IPAWS capability to aggregate and disseminate alerts. http://www.fema.gov/pdf/emergency/ipaws/ipaws_benefits_alert_%20authorities_factsheet.pdf

Cybersecurity

- ***WEA Service Cybersecurity Risk Management Strategy for Alert Originators –*** Software Engineering Institute report that describes the CSRM strategy in detail and provides example results from executing the strategy.

Developer Information

- ***Integrated Public Alert and Warning System (IPAWS) Webinar, Introduction to the New IPAWS-OPEN Developers Guide –*** FEMA site that offers an introduction and overview presentation on the IPAWS Open Platform for Emergency Networks (IPAWS-OPEN v3.01) Web-Service Interface Design Guidance, by Gary Ham, System Architect. http://www.fema.gov/library/viewRecord.do?id=5011
- ***OASIS Example Practices: CAP Elements Version 1.***0 **–** Provides example practices related to certain elements contained in CAP alerts, including CAP element usage and alerting challenges that impact CAP alerts. http://docs.oasis-open.org/emergency-adopt/cap-elements/v1.0/cnprd01/cap-elements-v1.0-cnprd01.pdf
- ***STEP [Supporting Technology Evaluation Project] –*** Information about a FEMA project managed by FEMA's Preparedness-Technology, Analysis, and Coordination (P-TAC) Center to conduct test and evaluation for technologies relating to incident management and response and to determine compliance. https://www.ptaccenter.org/step/index

Device Information

- ***Wireless Emergency Alerts on Your Mobile Device –*** CTIA–The Wireless Association provides a quick way to get information about cell providers and their WEA capabilities. CTIA is a nonprofit membership organization that has represented the wireless communications industry. http://www.ctia.org/consumer_info/safety/index.cfm/AID/12082

Education—Public Awareness

- ***Increasing Public Awareness About CMAS –*** A one-page discussion of approaches to educating the public on aspects of WEA, presented by Alerts, Warnings & Response to Emergencies with SRA International. http://www.awareforum.org/2012/07/increasing-public-awareness-about-cmas/
- ***Integrated Public Alert Warning System: Wireless Emergency Alerts –*** A two-page introductory piece to WEA by the Metropolitan Emergency Management Committee of Kansas City. http://www.jocoem.org/files/docs/WirelessEmergencyAlertFlier.pdf

Education—Technical

- ***Introduction to XML –*** A tutorial on XML (eXtensible Markup Language); XML is designed to carry data, not to display data, and serves as the format for WEA messages. http://www.w3schools.com/xml/xml_whatis.asp
- ***IS-247.A: Integrated Public Alert and Warning System (IPAWS) –*** Provides basic course and registration information for FEMA Emergency Management Institute's course on IPAWS. It includes benefits of using IPAWS for effective public warnings; skills to draft more appropriate, effective, and accessible warning messages; and best practices in the effective use of CAP to reach all members of affected communities. https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-247.a
- ***Start Learning SOAP Now –*** A tutorial to learn about SOAP, an XML-based protocol to let applications exchange information over HTTP. http://www.w3schools.com/soap/soap_intro.asp

Geotargeting

- ***Federal Information Processing Standard (FIPS)* –** U.S. Census Bureau (U.S. Department of Commerce) site that describes FIPS codes; used as of this writing as the minimum geotargeting requirement that carriers use for cell tower broadcasting. http://quickfacts.census.gov/qfd/meta/long_fips.htm

Standards and Tools

- ***About Web Content Accessibility Guidelines (WCAG) 2.0* –** Explains how to make web pages and web applications accessible to people with disabilities to maximize the ability of those with impairments to navigate the web. http://www.w3.org/WAI/flyer/handout2007b
- ***Common Alerting Protocol Version 1.2 OASIS Standard, 01 July 2010* –** Profile of the XML-based CAP; describes an interpretation of the OASIS CAP v1.2 standard necessary to meet the needs of IPAWS. http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf

Strategic Plan Examples

- ***Bay Area Emergency Public Information and Warning Strategic Plan* –** A publication of the Bay Area Urban Areas Security Initiative (UASI) in San Francisco, California, that outlines "the means by which the region's twelve OAs and three major cities can come together and develop a comprehensive five-year regional plan to strengthen regional EPI&W [Emergency Public Information & Warning] capabilities." http://bayareauasi.org/node/232

WEA Real-Time Use Examples

- ***Boston Bombing Shows How Wireless Emergency Alerts Can Work with Other Media* –** Blog describing the use of WEA messages in 2013 in the aftermath of the Boston Marathon bombing. The blog is sponsored by *Emergency Management*, an all-hazards publication for emergency-management, public-safety, and homeland-security stakeholders. http://www.emergencymgmt.com/emergency-blogs/alerts/Boston-Bombing-Shows-How-042313.html
- ***CMAS/WEA Used Extensively for Hurricane Sandy* –** Blog describing the use of WEA messages during Hurricane Sandy in 2012. The blog is sponsored by *Emergency Management*, an all-hazards publication for emergency-management, public-safety, and homeland-security stakeholders. http://www.emergencymgmt.com/emergency-blogs/alerts/CMASWEA-Used-Extensively-for-103112.html
- ***The National Weather Service Issues 3,185 WEA Alerts* –** Blog describing the use of WEA messages beginning in 2013 by the National Weather Service. The blog is sponsored by *Emergency Management*, an all-hazards publication for emergency-management, public-safety, and homeland-security stakeholders. http://www.emergencymgmt.com/emergency-blogs/alerts/The-National-Weather-Service-031313.html

Appendix H Acronym List

Acronym	Definition
AMBER	America's Missing: Broadcasting Emergency Response
AO	alert originator
CAP	Common Alerting Protocol
CMAS	Commercial Mobile Alert System; also, Commercial Mobile Alert Service, the former name of the Wireless Emergency Alerts (see also WEA)
CMSP	commercial mobile service provider
COG	Collaborative Operating Group
COTS	commercial off-the-shelf
CSRM	cybersecurity risk management
DHS S&T	Department of Homeland Security Science and Technology Directorate
DoD	Department of Defense
EAS	Emergency Alert System
EDXL	Emergency Data Exchange Language
EMA	emergency management agency
ENS	emergency notification system
EOC	emergency operations center
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
GUI	graphical user interface
HAZMAT	hazardous materials
IaaS	infrastructure as a service
IMS	incident management system
IPAWS	Integrated Public Alert and Warning System
IPAWS-OPEN	Integrated Public Alert and Warning System Open Platform for Emergency Networks
JITC	Joint Interoperability Test Command
LTE	long-term evolution
MOA	memorandum of agreement
MTW	Mission Thread Workshop
NCMEC	National Center for Missing and Exploited Children
NOAA	National Oceanic and Atmospheric Administration
NWS	National Weather Service
OASIS	Organization for the Advancement of Structured Information Standards
OPEN	See IPAWS-OPEN
OR	operational readiness
PaaS	platform as a service
PLAN	Personal Localized Alerting Network (former FCC term for CMAS; see also WEA)
PSAP	public-safety answering point
P-TAC	Preparedness-Technology, Analysis, and Coordination
QoS	quality of service
RACI	responsible, accountable, consulted, and informed
RDT&E	research, development, testing, and evaluation
RFP	request for proposal
SaaS	software as a service
SMS-CB	Short Message Service–Cell Broadcast

Acronym	Definition
SMS-PP	Short Message Service–Point to Point
STEP	Supporting Technology Evaluation Project
STRIDE	spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege
TR	technical readiness
URL	Uniform Resource Locator
WARN	Warning, Alert, and Response Network Act
WEA	Wireless Emergency Alerts
WSDL	Web Services Description Language
XML	eXtensible Markup Language

References

[Adolf 2011]
Adolf, S.; Hall, W.; & Kruchten, P. *A Methodological Leg to Stand on: Using Grounded Theory to Study the Experience of Software Development.* University of British Columbia, January 2011.

[Alerting Solutions 2013]
Advanced Warning Systems for Homeland Security and Infrastructure Protection. Alerting Solutions. http://www.alertingsolutions.com/welcome.html (2013).

[Bass 2012]
Bass, Len; Clements, Paul; & Kazman, Rick. *Software Architecture in Practice*, 3rd ed. Addison-Wesley Professional, 2012.

[Bay Area UASI 2012]
Bay Area Urban Areas Security Initiative. *2012–2017 Bay Area Emergency Public Information and Warning Strategic Plan*. Bay Area UASI, 2012. http://www.bayareauasi.org/sites/default/files/resources/Bay%20Area%20UASI%20EPIW%20Strategic%20Plan_0.pdf

[Caralli 2010]
Caralli, Richard A.; Allen, Julia H.; & White, David W. *CERT® Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience*. Addison-Wesley Professional, 2010.

[Cal EMA 2011]
California Emergency Management Agency. *SEMS/NEMS/ICS Combined Course Training Curriculum*. State of California, 2011. http://www.calema.ca.gov/csti/Pages/SEMS-NIMS.aspx

[Clements 2002]
Clements, Paul; Kazman, Rick; & Klein, Mark. *Evaluating Software Architectures: Methods and Case Studies*. Addison-Wesley Professional, 2002.

[CMMI 2010]
CMMI Product Team. *CMMI® for Acquisition, Version 1.3*. Carnegie Mellon University Software Engineering Institute, 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9657

[CFR 2012a]
Title 45: Public Welfare, Part 46: Protection of Human Subjects. *Code of Federal Regulations*. http://www.gpo.gov/fdsys/pkg/CFR-2012-title45-vol1/xml/CFR-2012-title45-vol1-part46.xml

[CFR 2012b]
Title 47: Telecommunications, Part 10: Commercial Mobile Alert System. *Code of Federal Regulations*. http://www.gpo.gov/fdsys/pkg/CFR-2012-title47-vol1/xml/CFR-2012-title47-vol1-part10.xml

[Corbin 2008]
Corbin, J. & Strauss, A. *Basics of Qualitative Research Techniques and Procedures for Developing Grounded Theory*, 3rd ed. Sage Publications, 2008.

[DHS S&T 2013]
Department of Homeland Security Science and Technology Directorate. *CMAS Integration Guidance Development* [webinar]. DHS S&T, July 19, 2013.

[Farrell 2013]
Farrell, Michael B. "Cellphone Networks Overwhelmed After Blasts in Boston." *The Boston Globe*. BostonGlobe.com, April 17, 2013. http://www.bostonglobe.com/business/2013/04/16/cellphone-networks-overwhelmed-blast-aftermath/wq7AX6AvnEemM35XTH152K/story.html

[FCC 2013]
Federal Communications Commission. *Wireless Emergency Alerts (WEA)*. FCC, 2013. http://www.fcc.gov/guides/wireless-emergency-alerts-wea

[FEMA 2012a]
Federal Emergency Management Agency. *IPAWS-OPEN v3.2 Web-Service Interface Design Guidance*, Version 3.02. FEMA, 2012.

[FEMA 2012b]
Federal Emergency Management Agency. *IS-247.A: Integrated Public Alert and Warning System (IPAWS)*. FEMA, 2012. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-247.a

[FEMA 2012c]
Federal Emergency Management Agency. *A State Toolkit for Adopting IPAWS*. FEMA, 2012. http://www.fema.gov/media-library-data/20130726-1831-25045-7105/state_toolkit_for_ipaws_adoption_20120320_final.pdf

[FEMA 2013a]
Federal Emergency Management Agency. *Alerting Authorities*. FEMA, 2013. http://www.fema.gov/alerting-authorities

[FEMA 2013b]
Federal Emergency Management Agency. *Integrated Public Alert and Warning System (IPAWS) Developer Webinar: Train, Drill, Exercise* [webinar]. FEMA, April 2013.

[FEMA 2013c]
Federal Emergency Management Agency. *IPAWS-OPEN v3.04 Web-Service Interface Design Guidance, Version 3.04*. FEMA, May 2013.

[FEMA 2013d]
Federal Emergency Management Agency. *National Incident Management System*. FEMA, 2013. http://www.fema.gov/national-incident-management-system

[FEMA 2013e]
Federal Emergency Management Agency, Preparedness-Technology, Analysis, and Coordination (P-TAC) Center. *Frequently Asked Questions*. https://www.ptaccenter.org/step/faq#q_20

[Gagliardi 2010]
Gagliardi, Michael J. *SoS Architecture Evaluation and Quality Attribute Specification.* Software Engineering Institute, Carnegie Mellon University, January 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=18682

[Glaser 2001]
Glaser, B. *The Grounded Theory Perspective: Conceptualization Contrasted with Description*. Sociology Press, 2001.

[IdeaScale 2012]
IdeaScale Corporation. *CMAS Research, Development, Testing, and Evaluation Forum* [online discussion]. IdeaScale Feedback Software, March 2012. https://cmasforum.ideascale.com/a/pages/about

[JITC 2011]
Joint Interoperability Test Command. *JITC Testing*. http://jitc.fhu.disa.mil/testing.html (2011).

[Landry 2013]
Landry, Alysa. "Indian Country Left on Far Side of Digital Divide." *The Navaho Times*, April 4, 2013. http://navajotimes.com/news/2013/0413/040413dig.php

[Lewis 2010]
Lewis, Grace. *Basics About Cloud Computing*. Carnegie Mellon University Software Engineering Institute, 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=28873

[Lewis 2011]
Lewis, Grace. *Architectural Implications of Cloud Computing*. Carnegie Mellon University Software Engineering Institute, 2011. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=18910

[Lewis 2012]
Lewis, Grace A. & Smith, Dennis B. *Four Pillars of Service-Oriented Architecture*. Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=29269

[NAS 2013]
National Academy of Sciences. *Workshop on Geotargeted Alerts and Warnings*. Washington, D.C., Feb. 2013. http://sites.nationalacademies.org/CSTB/CSTB_081131

[NIST 2013]
National Institute of Standards and Technology. *Federal Information Processing Standards Publications (FIPS PUBS)*. NIST, 2013. http://www.nist.gov/itl/fips.cfm

[NOAA 2013]
National Oceanic and Atmospheric Administration. *StormReady*. NOAA, 2013. http://www.stormready.noaa.gov

[OASIS 2004]
Organization for the Advancement of Structured Information Standards. *Web Services Security: SOAP Message Security 1.0 (WS-Security 2004).* OASIS Standard 200401. March 2004. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

[OASIS 2006]
Organization for the Advancement of Structured Information Standards. *Emergency Data Exchange Language (EDXL) Distribution Element, Version 1.0.* May 2006. http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf

[OASIS 2007]
OASIS Emergency Management Technical Committee. *Common Alerting Protocol v1.1*. https://www.oasis-open.org/standards#ditav1.1 (2007).

[OASIS 2009]
Organization for the Advancement of Structured Information Standards. *Common Alerting Protocol, Version 1.2 USA Integrated Public Alert and Warning System Profile, Version 1.0*. Oct. 2009. http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cap-v1.2-ipaws-profile-v1.0.pdf

[OASIS 2010]
Organization for the Advancement of Structured Information Standards. *Common Alerting Protocol, Version 1.2*. July 2010. http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf

[PMI 2009]
The Project Management Institute. *A Guide to the Program Management Body of Knowledge*, 4th ed. PMI, 2009.

[Riehle 2007]
Riehle, Dirk. "The Economic Motivation of Open Source Software: Stakeholder Perspectives." *IEEE Computer 40*, 4 (April 2007): 25–32.

[Santana 2013]
Santana, Marco. "Some Phone Companies Seek to End Landline Service." *The Des Moines Register*, March 31, 2013. http://www.usatoday.com/story/money/business/2013/03/31/phone-companies-seek-to-end-landline-service/2038743/

[SEI 2009]
Software Engineering Institute. *Systems-of-Systems Engineering*. Software Engineering Institute, Carnegie Mellon University, January 2009. http://www.sei.cmu.edu/sos

[SEI 2012]
Software Engineering Institute. *Commercial Mobile Alert Service (CMAS) Alerting Pipeline Taxonomy* (CMU/SEI-2012-SR-019). Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70067

[SEI 2013]
Software Engineering Institute. *Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators* (CMU/SEI-2013-SR-018). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70071

[Texas DPS 2013]
Texas Department of Public Safety. *About Emergency Management Exercises*. https://www.preparingtexas.org/preparedness.aspx?page=2cad08df-ffe5-4d67-9182-3a4ef8367bdf (May 2013).

[Trocki Stark 2013]
Trocki Stark, E.; Lavan, J.; Frankel, M.; Marshall-Keim, T.; & Elm, J. *Wireless Emergency Alerts: New York City Demonstration*. Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70024

[W3C 2007a]
World Wide Web Consortium (W3C). *SOAP Version 1.2 Part 0: (Primer) Second Edition*. April 2007. http://www.w3.org/TR/2007/REC-soap12-part0-20070427

[W3C 2007b]
World Wide Web Consortium (W3C). *Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language*. June 2007. http://www.w3.org/TR/wsdl20

[W3C 2008a]
World Wide Web Consortium (W3C). *Extensible Markup Language (XML) 1.0 (Fifth Edition)*. November 2008. http://www.w3.org/TR/2008/REC-xml-20081126

[W3C 2008b]
World Wide Web Consortium (W3C). *XML Signature Syntax and Processing (Second Edition)*. June 2008. http://www.w3.org/TR/xmldsig-core/

[Wimberly 2013]
Wimberly, Rick. “Boston Bombing Shows How Wireless Emergency Alerts Can Work with Other Media.” *Emergency Management Magazine Online*. e-Republic, 2013. http://www.emergencymgmt.com/emergency-blogs/alerts/Boston-Bombing-Shows-How-042313.html

[Wortham 2010]
Wortham, Jenna. “Data Networks Overloaded: New iPad Could Add to Slow Streaming.” *The Columbus Dispatch*. The Dispatch Printing Company, February 1, 2010. http://www.dispatch.com/content/stories/business/2010/02/01/cellphone_overload_nyt.ART_ART_02-01-10_A9_JHGF37K.html

[Yin 2002]
Yin, Robert. *Case Study Research: Design and Methods, 3rd ed. Volume 5, Applied Social Research Methods*. Sage Publications, 2002.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	February 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Study of Integration Considerations for Wireless Emergency Alerts	FA8721-05-C-0003

6. AUTHOR(S)

CERT® Division, Software Solutions Division

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-SR-016

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report supports the Wireless Emergency Alerts (WEA) program, formerly known as the Commercial Mobile Alert Service Research, Development, Testing, and Evaluation program, by identifying and analyzing key WEA adoption issues. The study captures key challenges for WEA message originators and offers recommendations to help the community avoid common pitfalls as it plans and implements the WEA service. The report summarizes the current strengths and challenges of WEA, how WEA fits into the alert originator's toolbox, and overall considerations for integrating a new WEA tool or service into an emergency management system as that system becomes ever more complex. The report also covers key topics for adopting a WEA tool or service, including requirements specification, cloud trends, cybersecurity, product selection, testing, coordinating among tools and alerting organizations, operational considerations, and alternatives to buying a WEA solution. For each of these topics, recommendations offer guidance that emergency management agencies can use to navigate the process of adopting and integrating WEA into their alerting capabilities.

14. SUBJECT TERMS	15. NUMBER OF PAGES
cybersecurity, emergency alerting, software acquisition, software integration, Wireless Emergency Alerts, WEA	131

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL